Centers for Disease Control & Prevention

Technical Review of Issues Related to Version 1 of the Public Health Information Network Functions and Specifications

FINAL Briefing

12 May 2003

Engagement: 220411890

research consulting measurement community news

Gartner

Agenda

- Background
- Engagement Overview
- Engagement Questions
- Findings Summary
- Analysis
- Recommendations
- Appendices
  - Interviewees
  - Industry Best Practice

Background

Engagement Overview
Background

- The Public Health Information Network (PHIN) will support specific IT functions that cross program boundaries and provide integrated services for an efficient public health information technology infrastructure. The PHIN will:
  - Build IT capabilities and capacity through all levels of public health (local, state, and federal) to serve the variety of public health programs and functions.
  - Ensure public health IT works as a coherent network and has the ability to connect to other groups (i.e., clinical care, law enforcement).
  - ***Implement and verify specific industry standards and to develop specifications internally to those standards:***
    - ***to ensure comparable data, information exchange and interoperable systems; and***
    - ***to facilitate the management, retrieval and delivery of public health information (i.e., reference, educational and communications).***
  - Develop information and knowledge resources to educate and inform the public, public health personnel, and the health care workforce.
  - Research and evaluate electronic approaches that can further complement the capabilities of public health professionals in identifying and responding to public health event and trends.
  - Strengthen the technical capabilities of the public health workforce to implement and support reliable, interoperable technology solutions.
  - Provide technical assistance and support to public health partners in pursuit of these goals.
  - Evaluate network functionality and ensure interoperability, security, and reliability.

Engagement Overview
Background (Continued)

- The PHIN will be a live, secure, Internet-based network for exchanging comparable critical health information between all levels of public health (local, state and federal) and other critical information systems (clinical care, laboratories, first responders, etc.). The PHIN will connect the diverse groups participating in public health using standards-based collaboration, communications and alerting capabilities. Improved data analysis and visualization including automated algorithms for event detection will aid in more timely public health decision-making.
- The CDC Information Council (CIC) took an important first step in April 2002 by deciding that CDC would work to adopt IT standards and specifications that would apply to all CDC information technology initiatives that operate in, or interact with the national public health infrastructure. The urgency and compressed time frame required for the bioterrorism (BT) cooperative agreement did not permit a full process for evaluation and review of the functions and specifications that were attached to it. As potential CDC enterprise wide standards, their heavy reliance on NEDSS and Health Alert Network (HAN) standards and their presence in the BT guidance made them a reasonable starting point for CDC enterprise wide standards.
- In August 2002, the CIC approved these standards as Public Health Information Network Version 1 Functions and Specifications as well as approving an ongoing process for their review and evolution. In this process, several questions / concerns were raised. Therefore, the CIC also requested ***an initial technical evaluation of the PHIN functions and specifications in the context of the questions / concerns and requested that this review be completed as soon as possible*** to insure that public health organizations can wisely invest resources that are now available in the adoption of these standards.

What is a Public Health Information Network?

- The Public Health Information Network is an electronic nervous system that supports monitoring and maintaining the public's health. Like the human nervous system, it will detect problems, analyze accumulated data, create useful information, communicate alerts as needed, and direct appropriate responses to maintain health.

- Vision of Public Health Information Network: One information network that integrates, functionally and organizationally, public health partners across the nation. This is a dual use platform and a foundation to handle routine public health activities, bioterrorism detection and response, as well as new IT applications, as we pursue the objectives of public health.

Source: CDC

Public Health Information Network Requirements

- An interoperable network—built on the Internet and using industry standards to work with other networks / systems
- Support users—provides information and decision support to the public and public health professionals at all levels
- Live data—continuous monitoring of nations health, continuous detection and evaluation of threats
- Dual use—will meet BT preparedness and response needs and will transform routine public health practice
- Engage industry—set direction for private sector participation and develop commercial and clinical opportunities
- A common data language—use of industry standards for comparable data use and exchange (HL7, SNOMED, LOINC)

Source: CDC

Public Health Information
"Live" Network

"Live" Exchange of and Access to Specific Data for Interoperable Systems – Messages and Storage

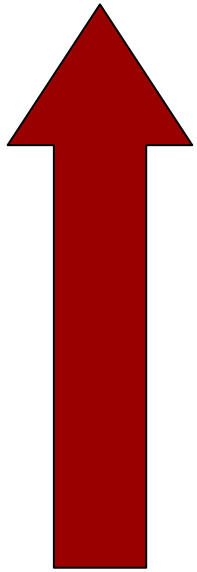
Specific Data Content – Vocabulary and Implementation Guides (LOINC, SNOMED, etc.)

Data Structure – Data Models (PHLDM, HL7 etc.)

Transport / "Handshake Between Information Systems" - ebXML

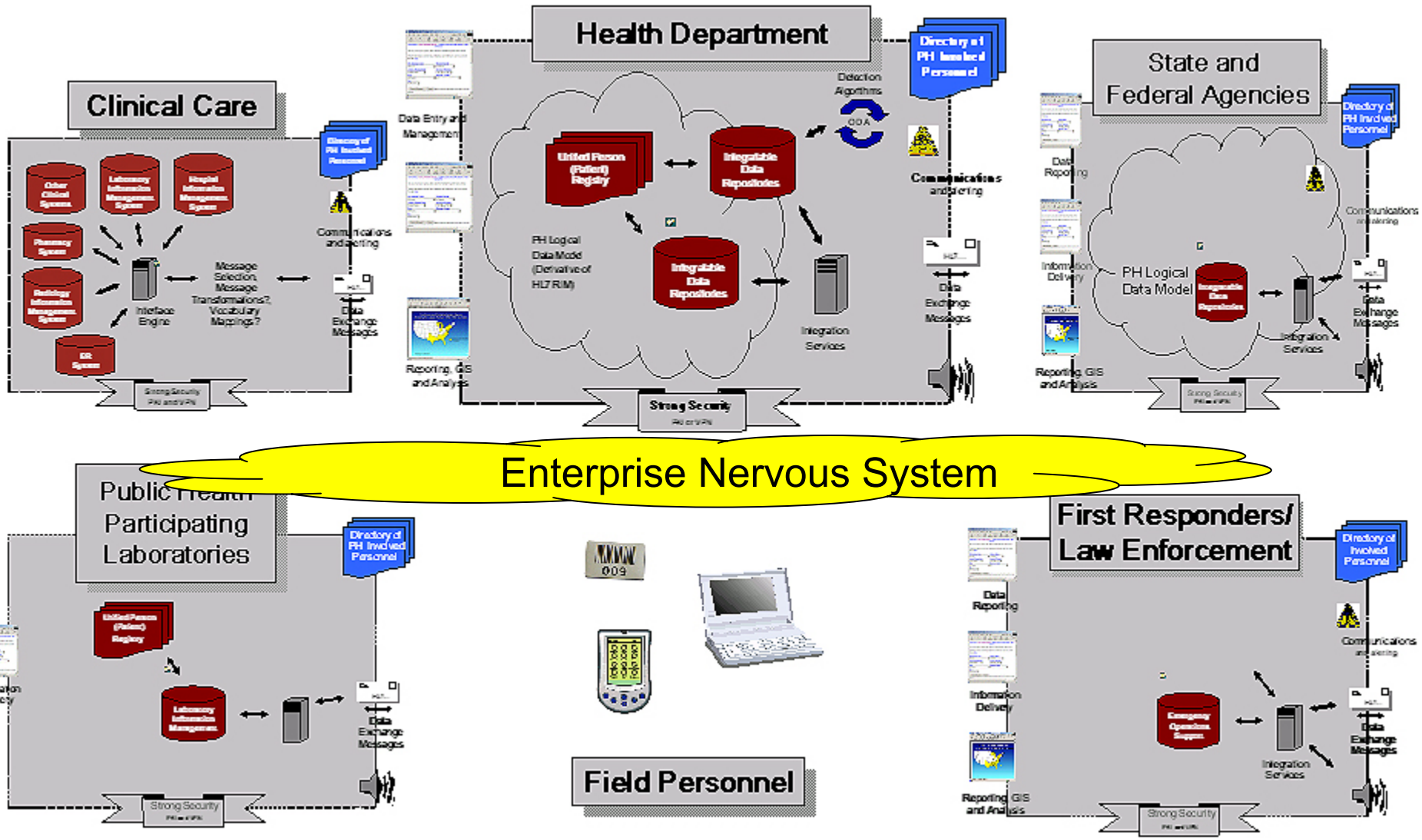
Encryption / Security – HTTPS, PKI

Connectivity – Continuous Internet Connectivity



Source: CDC

Public Health Information Network



Initiatives Spearheading the PHIN

- **Specific CDC initiatives have demonstrated the value of public health information technology:**
  - Health Alert Network (HAN)—Internet connectivity, alerting and distance learning
  - National Electronic Disease Surveillance System (NEDSS)—disease surveillance, electronic laboratory reporting
  - Laboratory Response Network (LRN)—diagnostic capacity and information delivery
  - Epidemic Information Exchange (EPI-X)—Secure, interactive communications
  - CDC Web Site Redesign—Public information access and public health education

- **Now that public health is being tested by new needs for preparedness and response, it is time to advance a unified information technology framework for these and other activities.**

Source: CDC

Engagement Overview

Engagement Overview
Goals & Objectives

This engagement has the following goals & objectives:

- **The CDC would like to engage an independent third party to conduct the review of issues related to Version 1 of the Public Health Information Network (PHIN) standards. This engagement will build on the NEDSS technical architecture compliance work already completed for the CDC.**
- **The objectives for this effort, as we understand them, are as follows:**
  - Conduct a review of the PHIN functions and specifications (Version 1) in relation to the questions and issues that have been raised by the CIC and its partners;
  - Provide an analysis report in both draft and final versions; and
  - Deliver the final report to the CIC External Technical Standards Working Group.

Engagement Overview
Approach and Methodology (Cont'd)

- **Task 1. Conduct Kickoff Meeting**
  - Conducted a meeting to organize the engagement, establish roles & responsibilities and perform initial data collection.
- **Task 2. Perform Data Discovery**
  - Conducted interviews and reviewed documentation for PHIN and related initiatives.
- **Task 3. Conduct Research and Findings Analysis**
  - Assessed findings, conduct research and develop initial conclusions.
- **Task 4. Develop Draft & Final Report**
  - Developed a working draft of the assessment results and "working conclusions" and reviewed with project team.
- **Task 5. Deliver Final Briefing**
  - Deliver final management briefing to the project team and key stakeholders in CDC.

Engagement Questions

Engagement Questions

Task 3 Questions

- Is ebXML the right standard for the secure real-time, bi-directional exchange of public health messages across the Internet? Are there issues interfacing ebXML software with organizations that are using Microsoft software internally?
- Is LDAP/LDIF the right industry standard for interoperable directory services?
- What are the implications for application servers, regardless of physical platform, to run shared Java code? If the goal is to be able to have one version of an application run in any environment is there a way to have Microsoft application code be used in that context too?
- Do any of the functions and specifications mandate a particular product that might conflict with existing jurisdictional standards? Are there approaches to mitigating any conflicts, while still maintaining the functional objectives of the standards?
- Provide a realistic timeline for implementation of all the functions and specifications. (Consider some jurisdictions are starting from very basic IT functionality).
- Describe how participants can incrementally move toward compliance.
- Is there a sequence in which the functions and specifications should be implemented? How does the national mandate for bioterrorism preparedness get impacted by this sequence?
- How will those jurisdictions that are “behind” or “ahead” be supported while others “move further ahead”?
- Provide a clear definition of “compliance” which can provide a means by which our partners can assess (or self-evaluate) their systems for compliance with PHIN standards.
- Review for accuracy and provide clarifications if needed to the definitions in the glossary. Terms of particular interest include: LDAP, SMTP, Web Services, Multi-Tiered Architecture, ebXML, JavaScript, Microsoft Active Directory Services, and Firewall.

Engagement Questions

Questions Regarding the PHIN Version 1

- **Direct questions from both internal CDC groups and the Public Health partners:**
  - What are the Systems Integration Components to which the states should map?
  - What are the processes to review and vet the PHIN standards and specifications moving forward?
  - What are the overall Governance processes to support the PHIN program at CDC?
  - What is the CDC Enterprise Architecture (EA)?
  - What are the supporting processes for the CDC's EA?
  - How can we simplify the PHIN document and make it more clear?
  - How can we clean up the reference material to make it more clear?
  - Aren't some of these IT capacities really public health functions?

- **Questions from the interviews:**
  - How do State & Local public health partners achieve interoperability with the PHIN?
  - What do you have to do to write cross-platform services?
  - Is it necessary to run Java modules to be compliant?
  - Why is CDC advocating programming languages (i.e., Java) for an integration architecture?
  - What standards are in use today and what are visionary?
  - What is the "state of the market" for these proposed technologies?
  - Should CDC be advocating ebXML or more widely used transport standards found in use in public health (e.g., VPN, encrypted email, secure FTP, etc.)?
  - Should the CDC be developing its own version HL7 3.0 message segments (ahead of industry) or should they be advocating existing v2.x message segments and wait for industry to drive to the next release?

Findings Summary

Findings Summary
From Interviews—General

- **The vision and mission of the PHIN is widely accepted by the public health (PH) partners as correct…everyone buys into the concept of the PHIN.**
- **The PH partners feel that the PHIN will help establish new standards and guidelines for each of them to use in building and integrating their systems and data. The PHIN is a foundational "road map" for systems integration.**
- **Not all of the most current "mission, vision, program charter, etc." material on the PHIN is readily available on the Web.**
- **The PH partners see PHIN as the continuing evolution of NEDSS activities—with an emphasis on systems integration.**
- **The PHIN vision must continue to broaden beyond the structured data obtained from surveillance systems and labs to include syndromic data from clinics, ERs, Doctor's offices, pharmacies, etc. that may not be available in a structured form.**
- **The PHIN has not adequately addressed the details of how to capture early warning or emergency response data that could be gathered from a variety of less structured sources and systems—the "access architecture" must continue to be broadened to address multiple means of data entry when a PHIN compliant surveillance system, process or web based interface is not available.**

Findings Summary
From Interviews—General

- **Controlled medical vocabularies (CMVs) are evolutionary in nature. The PHIN needs to accommodate reporting on data where codes have not been established.**
- **There is a lack of governance and process at the CDC to support the continued development and review of these standards—to include input from all partners. These items need to be developed for long term support of the PHIN and the PH partners must participate to help achieve this.**
- **There are still some PH communities (outside of CDC and PH partner control, but part of the overall "PHIN") not using HL7 messaging formats, even in the advent of organizations such as the National Committee on Health and Vital Statistics (NCHVS), the Consolidated Health Informatics (CHI) initiative and HIPAA regulations advocating its use.**
  - HHS Secretary Thompson's announcement on 23 March 03 specifically called for all federal agencies ***to adopt Health Level 7 messaging standards***, certain National Council on Prescription Drug Programs standards, the Institute of Electrical and Electronics Engineers 1073 series of standards, the Digital Imaging Communications in Medicine standards and ***the laboratory Logical Observation Identifier Name Codes (LOINC)***.

Findings Summary

From Interviews—Internal to CDC

- **Currently, CDC software development (for both distribution to PH partners and internal use) is on a variety of platforms representing different architectural "design patterns". There is concern that the PHIN/NEDSS standards are going to become a "one size fits all" development solution for all business needs.**
- **For the internal shops that are developing in an J2EE environment, there is little to no impact adopting these standards.**
- **For internal shops developing in .NET, DCOM or other environments, there is a huge impact (time, resources and money) to develop in the J2EE "design pattern" because of investments already made in other systems and skills.**
- **There is no consistent application of SEI CMM* like processes at CDC for developing systems. Applications Development may not be a core "business" of the CDC, but a tremendous amount of resources have been invested in it. Several examples encountered by Gartner at the CDC include multi-million dollar per year projects with a wide variety of development process, tools and skill.**
- **There is a serious lack of architectural management across the CDC—each center and each vendor employed brings in "their own architecture".**

*Software Engineering Institute Capability Maturity Model

Findings Summary
From Interviews—External to CDC

- **PH departments' biggest concerns today are regarding the mandates for HIPAA compliance with the protection of client sensitive data (i.e., privacy) and the threats / implications of bioterrorism.**
- **States see PHIN as more of a conceptual plan for the PH departments to follow than a detailed road map for application development.**
- **States see PHIN as defining an integration architecture, not an application architecture (i.e., emphasis on data standards, formats and communication).**
- **Most states are supporting a variety of "low tech" HW/SW platforms today (applications and networks) to communicate information from local PH entities and clinical partners to state PH departments.**
- **Most PH departments are using some form of directory services (not necessarily LDAP). Very little LDAP capability is in place today.**
- **Very little HL7 capability is in place today. Mostly this is used with large "trading partners" such as national labs.**
- **States have developed software using a variety of development environments including .NET and Java; additionally—Visual Basic, FoxPro, etc.**

Findings Summary
From Interviews—External to CDC Continued

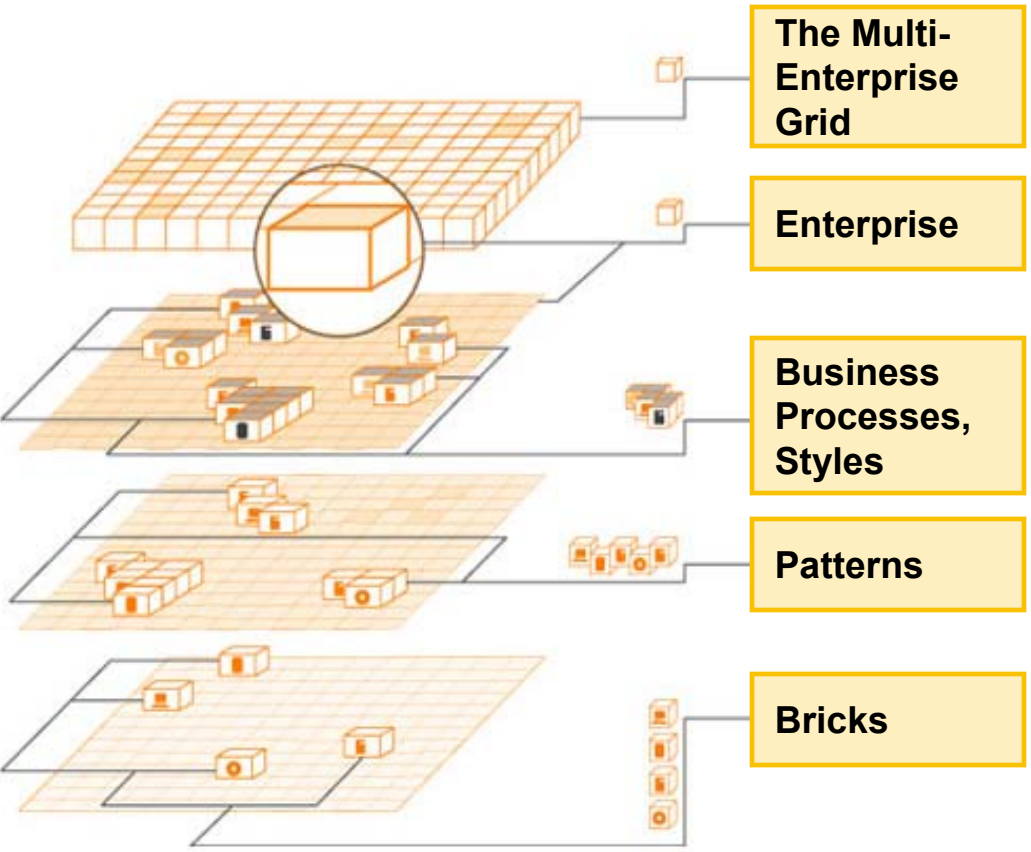
- There has been some reaction to the requirement to provide the ability to run "shared Java code" on partner owned platforms (no matter what they are).
- There were several requests for the NEDSS Base System roll out to individual states—there is a real desire for this product in the field.
- State PH partners feel that the PHIN should be focused primarily on data, data formats, data elements—and less on future technologies such as ebXML. The states would like to see more work on the data formats, CMVs and how to structure that data for transmission.
- HL7 is too expensive for most labs to implement within their Laboratory Information Management Systems (LIMS)—they would like to see CDC develop a LIMS or put money into a commercial product to give to the states that meets the PHIN standards.
- States want more communication on the PHIN functions/topics in order to build out this proposed infrastructure. For example, how is LDAP truly to be implemented and securely used for the national "Directory of Public Health"?

Findings Summary
Documentation Review

- **Documentation Reviewed:**
  - PHIN Functions and Specifications Version 1.2, 18 December 2002
  - Appendix to PHIN v1.2 - Comments/Questions/Answers from CIOs
  - PHIN Functions and Specifications Glossary v1.2, 18 December 2002
  - NEDSS Notification Messaging, v1, various dates
    - Summary Disease Reporting Implementation Guide
    - General Disease Implementation Guide
    - Sexually Transmitted Diseases Implementation Guide
    - Rubella Implementation Guide
    - Congenital Rubella Syndrome Implementation Guide
    - Hepatitis Implementation Guide
    - Pertussis Implementation Guide
    - Bacterial Meningitis Implementation Guide
    - Measles Implementation Guide
  - CDC Web Site material
    - e.g., CDC IRMO Information Technology (IT) technical and direct assistance services
  - NEDSS Program specifications and related material
  - Material provided by State partners on messaging and other related matters
  - HL7 Specifications for Electronic Laboratory-Based Reporting of Public Health Information, 1 Oct 1997
  - Gartner Research and Consulting Material

Gartner's Architecture Framework

Gartner's approach to Architecture begins with a conceptual framework that includes Grids, Styles, Patterns and Bricks. The Grid is a logical framework that establishes the universe of discourse including the definition of the enterprise, the virtual enterprise, the applications universe, the network and other necessary common understandings.

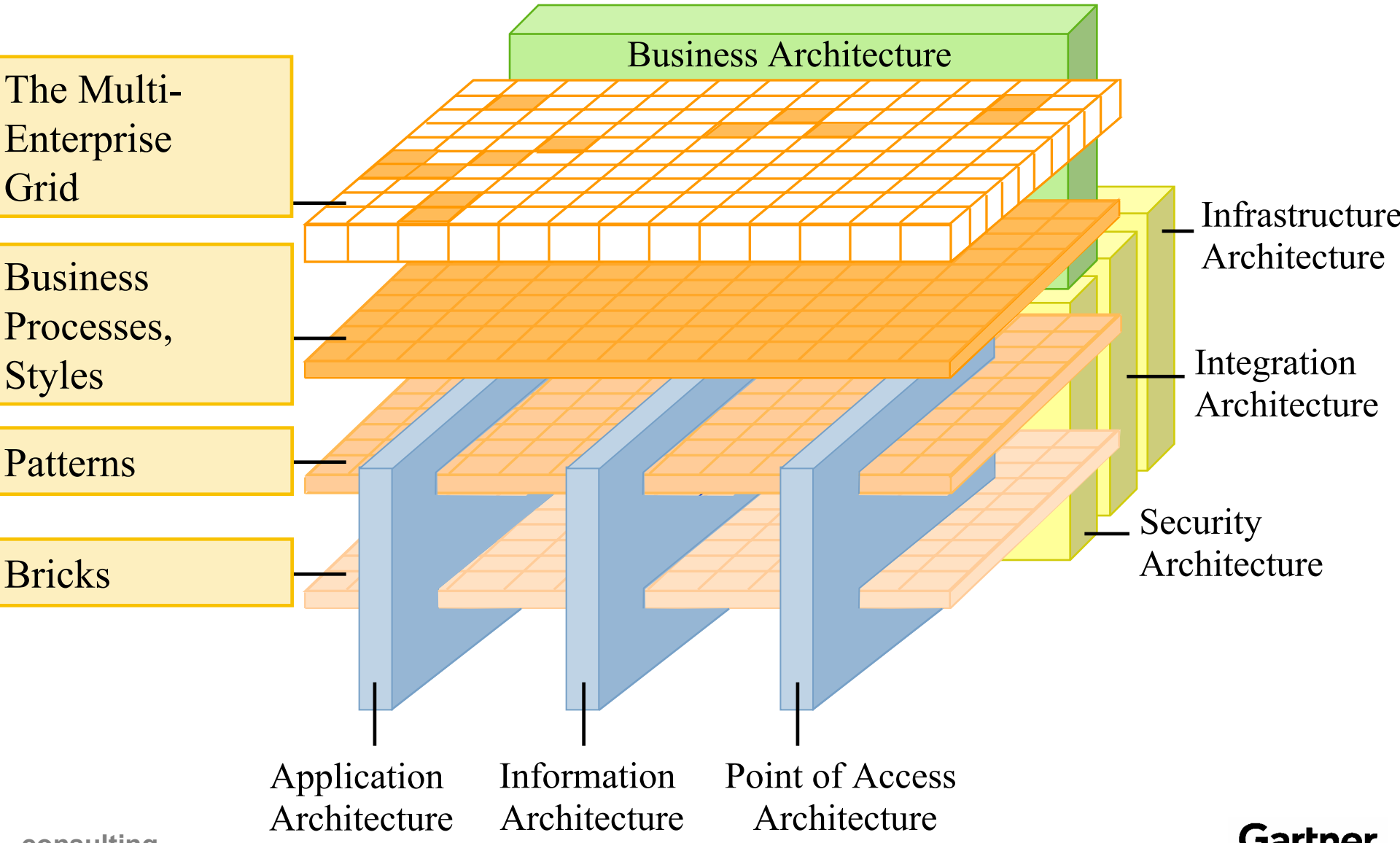


Styles are modes of processing such as transaction processing (OLTP), real-time, collaborative, analytical, and utility processing. Styles include the business activities, not just technology.

Next, Gartner's framework includes design patterns -- architectural models that show a logical view of the technology implementation of the the Styles.

At the lowest level are the elemental "bricks", fundamental building blocks, which are organized according to a formal taxonomy in the Technical Reference Model.

Gartner's Architecture Framework



When Someone Says "Architecture"
What Does They Mean?

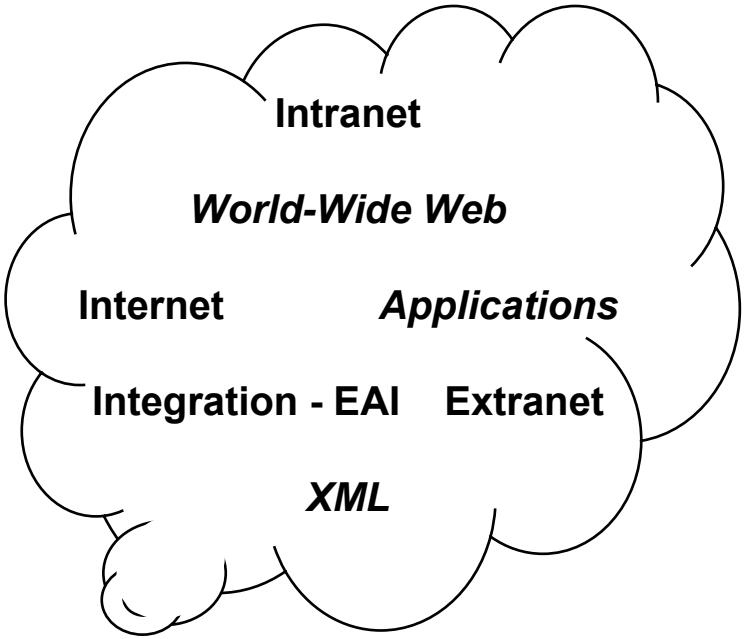
- **The term is not used the same way everywhere. It may imply any of the following …**

1. Kinds of architecture:

- application architecture
- network architecture
- middleware architecture
- object/component architecture
- **integration architecture**
- technical architecture
- **web (Internet / Intranet) architecture**
- **e-business architecture (B2C & B2B)**

2. Scope:

- project
- **enterprise**
- consortium
- etc.



Analysis

- **Q: Is ebXML the right standard for the secure real-time, bi-directional exchange of public health messages across the Internet? Are there issues interfacing ebXML software with organizations that are using Microsoft software internally?**
  - The ebXML Message Handling Service specification was originally developed by the ebXML initiative of UN CEFACT. At the completion of that initiative the specification was turned over to OASIS which has continued to maintain and extend the specification. Version 2.0, the ebMS (Messaging Service) was approved by OASIS in April 2002.
  - ebMS provides Confidentiality, Authentication, Integrity of the Message, and Non-repudiation (CAIN) functionality for payloads in any syntax.
  - The only similar standard is a draft of the IETF, generally referred to as EDIINT AS2. EDIINT handles EDI explicitly, but only handles HL7 in an “other” category.
  - The Web Services community is developing WS-Reliability specifications which may have similar capability.

- **Q (continued):**
  - Both ebMS and EDIINT AS2 have had successful interoperability testing, involving a limited number of software agents running in the Windows and other operating systems.
  - Neither has progressed to the point where two arbitrarily chosen compliant program agents would interoperate without tweaking.
  - Both protocols have been used successfully by channel masters that either (a) offer downloadable communications software to trading partners, or (b) offer a certification program to support trading partners in tweaking their software for interoperability.
  - ebMS is based on a variation of SOAP which makes it closer to Web Services
  - The OASIS group working on ebMS has stronger ties with the Web Services community and is more likely to converge with WS-Reliability as it evolves.
- **A: Yes - ebMS is an appropriate protocol for the PHIN to target for adoption.**
  - Neither protocol is ideal, but each has been proven viable in controlled environments.
  - However, the evolutionary path of ebMS allows for better alignment with the widely proliferated Web Services initiatives.

- **Q: Is LDAP / LDIF the right industry standard for interoperable directory services?**
  - LDAP is a directory access methodology that can be used to access conventional directories (such as Microsoft Active Directory, Novell eDirectory and Sun ONE Directory Server), as well as relational databases and other data structures. LDAP describes the access methodology but not the underlying store. **In most respects, LDAP is to directories what Open Database Connectivity (ODBC) is to databases.**
  - LDAP directories are highly scalable. They can easily support millions of users and can be implemented in a centralized or decentralized architecture.
  - LDAP directories are streamlined for reading. In most cases, an LDAP directory will outperform a database when it comes to heavy read loads.
  - LDAP directories are supported by third-party vendors. This makes it easier to bring in a third-party application or authentication module and integrate it into your infrastructure.
  - LDAP is a simple standard for programmers to implement. Using LDAP insulates programmers from platform and vendor tie-ins.
- **A: LDAP is the appropriate for use within the PHIN.**

Analysis
Task 3 Questions

- **Q: What are the implications for application servers, regardless of physical platform, to run shared Java code? If the goal is to be able to have one version of an application run in any environment is there a way to have Microsoft application code be used in that context too?**
  - Running shared Java code, regardless of physical platform for the application servers, is an unnecessary burden to place on the State and Local partners. The CDC should mandate internal coding platforms and standards as part of its enterprise architecture design pattern for software being released to its PH partners.
  - EA design patterns for PHIN can be provided as guidance to the PH partners, but the PHIN will focus on data, data structure and communication standards for its partners.
- **A: The key here is "policy" versus "guidance". CDC should mandate use of these application development standards as policy for internal CDC development and provide them as guidance to partners.**

Analysis
Task 3 Questions

- **Q: Do any of the functions and specifications mandate a particular product that might conflict with existing jurisdictional standards? Are there approaches to mitigating any conflicts, while still maintaining the functional objectives of the standards?**
  - This question is really only answered by a complete state by state assessment (not part of this engagement).
  - Anecdotally, through the interview process conducted for this review, these functions don't appear to conflict with any known jurisdictional standards.
  - An additional insight to this question though is to what extent is this question relevant if the focus of PHIN will be on systems integration standards (and not on specific implementation approaches as discussed on the previous slide)?
- **A: The PHIN standards should focus on systems integration components (data exchange, formats and secure transmission) for state partners as recommended in this report.**

Analysis

Q: A realistic timeline for implementation...

- **A: A realistic implementation guideline for PHIN would include the following:**
  - Gartner makes no assumption of a particular programming language or development environment mandate for external CDC application development, but assumes CDC will continue to publish "guidance" by way of PHIN standards and specifications documents.
  - Gartner assumes that the CDC will promote not only the PHIN/NEDSS standards for application development, but will allow for a transitional elements within that architecture. The transitional components are for those architectural elements that are not widely available in the commercial market or are too burdensome for the PH partners to implement throughout the partner "supply chain" at the present time. Further discussion within industry best practices section...
    - Note: CDC and partners should perform a quick "technology survey" with the States to understand the current baseline of architectural components and standards in use and to determine what compliant components may be leveraged by the PHIN
  - If the CDC mandates use of the PHIN/NEDSS standards for internal CDC application development, AD time will increase for those shops currently on different architectural platforms.
  - Generally speaking, a well-resourced AD shop can develop basic application functions / capabilities using a PHIN compliant data model, CMVs, directory services, messaging formats, transport & security standards, etc. (through either internal staff or contractors who have these skills) within 9-12 months - longer for those shops that will need training on these components.
  - Any major systems re-architecting (by internal CDC, State, or Local partners) will depend on the size and scope of the required changes. For example, a system requiring a messaging only addition should be able to comply within 3-6 months. A large system that does not currently use a compatible data model or CMVs may take as much as 18-24 months to re-architect.
  - The CDC and its PH Partners need a real commitment to do this!

Analysis

Q: The incremental steps towards compliance...

- **A: The incremental steps towards compliance would include adoption of a transitional architecture and supporting processes by CDC (see industry best practice section):**
  - With the adoption of transitional architecture elements (i.e., those items that are widely used in industry but do not represent the "target architecture"), the CDC and its PH partners must ensure that the transitional elements guarantee similar features and security (e.g., guaranteed delivery of messages and maintaining the goal of a "live" network) and that there is a plan to migrate to the target architecture within a reasonable timeframe.
  - The CDC can promote the adoption of the target architecture by buying or building compliant components such as an HL7 compatible LIMS and messaging systems (available from CDC today as prototypes—such as the PH Messaging System) and providing this to its PH partners. Additionally, CDC could provide PHIN compliant code to COTS vendors to include in their products.
  - To move towards compliance, if at all possible, these activities should be undertaken concurrently.
  - If resources are constrained, application development teams should focus first on the data, data structure, data model and the use of CMVs in their applications (i.e., create data that can be easily aggregated at the national level using the XML schema).
  - The next series of activities should focus on the development the messaging formats, transport & security standards to easily and securely share this data with its PH partners and CDC.
  - Then, focus on directory services that will allow authorized and controlled access to provider information should be developed and made available to the PHIN.
  - Lastly, anything that can be provided by CDC (e.g., compliant software modules, tools for messaging, etc. built on PHIN standards) should be made available to the states and their partners in an effort to develop a nationally compliant PHIN infrastructure.

Analysis

Q: The sequencing of these steps...

- **A: The sequencing for PHIN functions should be:**
  - Data: data structure, data model and the use of CMVs in their applications (i.e., create data that can be easily aggregated).
  - Messaging: formats, protocols and message segments.
  - Transport: transport & security standards to share this data.
  - Directory services: Allow for authorized, controlled and secure access to provider information nationally.

Analysis
Q: For those ahead or behind...

- **A: For jurisdictions moving "ahead" or "behind":**
  - No architecture ever has everyone "on the same page".
  - The "target" systems integration architecture (i.e., PHIN) must provide standards, design patterns and formats that application developers use to integrate their applications into the PHIN.
  - For particular components, CDC should provide the tools and modules to help promote standards and build out key PHIN infrastructure components (e.g., HL7 v3.0 structures, ebXML messaging, etc.).
  - PHIN should allow for multiple solutions for those components that are more technically challenging or immature in the market - with the goal of annual review and updating of these solutions through the EA Core Processes (e.g., HL7 v3.0, ebXML). However, the goal of a "live" network must be maintained.
  - Where jurisdictions are ahead they are less able to leverage what CDC can provide, but they must be seen as a valuable input to CDC's contribution (potentially the new "target" architecture). See Industry Best Practices Section for EA Core Processes - Exception Handling Process.
  - For those that are behind, CDC should provide tools that allow them to work at their level of technical competence in a secure and reliable manner and strive to maintain the goal of the "live" network.
    - For example: information transfer could function like a clearing house (i.e., the state PH department is the clearing house for the state and its partners) :
      - » larger organizations and the state PH department employ the PHIN standards for communication;
      - » mid-size organizations or larger local jurisdictions use electronic, but alternative transfer standards (e.g., secure FTP, encrypted email, etc.) - guaranteed to delivery standards; and
      - » small organizations, small jurisdictions accomplish data entry via web to State or rely on alternative processing until this capability is available.

Analysis
Task 3 Questions

- **Review for accuracy and provide clarifications if needed to the definitions in the glossary. Terms of particular interest include: LDAP, SMTP, Web Services, Multi-Tiered Architecture, ebXML, JavaScript, Microsoft Active Directory Services, and Firewall.**
  - Gartner has reviewed the glossary and updated it as appropriate (39 pages) - see attachment.
- **Provide a clear definition of "compliance" which can provide a means by which our partners can assess (or self-evaluate) their systems for compliance with PHIN standards.**
  - A PHIN Compatible System will meet all the standards provided within the specifications. Gradations of compatible may need to be considered during evaluation.
  - Compliance Testing will evaluate specific elements of systems to function within the PHIN specifications and will focus on applications that can create and send data in the correct format through the agreed to business rules that supports the "live" network in a secure, reliable, near real-time, and resilient manner.
- **Review for accuracy and provide clarifications if needed to the definitions in the glossary.**
  - Glossary attached.

Analysis
Written Questions from Partners

- **Questions regarding Release 1 of the PHIN from both internal CDC groups and the Public Health partners centered around several consistent themes:**
  - What are the Systems Integration Components to which the states should map?
  - What are the processes to review and vet the PHIN standards and specifications moving forward?
  - What are the overall Governance processes to support the PHIN program at CDC?
  - What is the CDC Enterprise Architecture (EA)?
  - What are the supporting processes for the CDC's EA?
  - How can we simplify the PHIN document and make it more clear?
  - How can we clean up the reference material to make it more clear?
  - Aren't some of these IT capacities really public health functions?
- **A: Answered in industry best practice and recommendation sections.**

Analysis
Questions from Interviews

- **The following questions/themes were brought up during the interview process for this engagement:**
  - How do State & Local public health partners achieve interoperability with the PHIN?
  - What do you have to do to write cross-platform services?
  - Is it necessary to run Java modules to be compliant?
  - Why is CDC advocating programming languages (i.e., Java) for an integration architecture?
  - What standards are in use today and what are visionary?
  - What is the “state of the market” for these proposed technologies?
  - Should CDC be advocating ebXML or more widely used transport standards found in use in public health (e.g., VPN, encrypted email, secure FTP, etc.)?
  - Should the CDC be developing its own version HL7 3.0 message segments (ahead of industry) or should they be advocating existing v2.x message segments and wait for industry to drive to the next release?
- **A: Answered in analysis, industry best practice and recommendation sections.**

Analysis
Gaps in the PHIN?

- **It appears that the following elements are missing or not fully developed in version 1 of the PHIN:**
  - The architecture needs to be more specific on the “analytics” component. How is data to be analyzed at the CDC? Is data stored in a data warehouse? data marts? How do states access their information? How do other constituents access this data and use analysis and visualization tools?
  - The architecture needs to describe any “collaboration” components such as message boards, white board capabilities, etc.
  - Continue to develop the “PH Information Dissemination and Alerting” function through a look at the “enterprise nervous system” technologies that are immerging.
  - The PHIN needs to fully develop the business continuity planning / disaster recovery components of this architecture. How resilient is the architecture in case of failures of individual data bases, network segments, etc.? Should key states have alternative communication paths to CDC other than the internet?
  - What are the databases of record that make up the PHIN? Who manages them?
  - How are non-structured data (e.g., some of the syndromic data) to be viewed? searched?
  - The security standards (beyond message transport) need to address items like overall information assurance program, denial of service attacks, cyber terrorism, etc.

Recommendations

Recommendations
Summary

- **Fully Develop EA, EA Governance structure and processes:**
  - Emphasize Systems Integration components to PH partners—data, data formats, CMVs, messaging, secure PH directory, secure transport—not development languages/platforms.
  - Establish PHIN v1 as the target architecture, establish Standards Review and Exception Handling processes for PH partners (perform a quick technology survey and component review to support this effort)
  - Make accommodations for "transitional" architectures to reflect state of the market for certain technologies and PH partner technical competence. Ensure that there is a plan and a timeframe to migrate to the target architecture.
  - Structure PHIN documentation to better communicate its systems integration mission externally and AD standards internally
  - Continue to provide detailed specifics on the technical standards to PH partners and continue to provide support from CDC technical resources to enable them.
  - Address the architecture "gaps" identified in this report.
- **Develop and release compliant modules for PHIN, make available to PH partners.**
- **More fully develop the implementation guidelines, development tool kits and AD maturity processes—policy for internal CDC and as guidance for PH partners.**
- **Develop PHIN compliance capability through self accreditation process, IV&V, test data sets and materials.**
- **Develop a communication strategy / marketing campaign to ensure that the right documents get to the right people.**
- **Clearly identify databases of record and establish appropriate data management practices.**
- **Develop BCP/DR strategy and test.**

Recommendations
Summary

- **Develop EA Governance structure and processes:**
  - Implement the EA governance structure and processes found in the industry best practices section.
  - Continue to promote input from all PH partners in a structured fashion through these processes.
  - Institute a software engineering discipline at CDC—ensure that no money is spent for systems development until the architecture is reviewed and approved by the sponsoring center and the larger governance framework at CDC.
  - Fully develop Office of the Chief Architect and and the IT Architecture team at CDC.
- **Develop a formal CDC EA that includes PHIN:**
  - EA will encompass all of CDC's architectural needs, it will have multiple design patterns for different business problems
  - There will not be a "one size fits all" solution for an enterprise as diverse as CDC
  - PHIN/NEDSS will be a component of this architecture and provide design patterns for surveillance systems internally developed at CDC
  - PHIN will provide the integration components to which all public health partners will adhere and application development "guidance"
  - Need to develop transitional architectures to the lowest common denominators, evolve and move forward with partners and the market. Include a "plan of actions and milestones" (POA&M) and a commitment to migrating to the target architecture in a reasonable timeframe.

Recommendations
Summary

- **Structure the PHIN documentation to better communicate its systems integration mission:**
  - The nine functional categories can be left as a business architecture or “business model” for the health professionals
  - Reorganize the 9 functional categories to 5 (see below) for the technical teams to provide the IT guidelines; reorganize the categories and remove redundancy in the specifications; put this in more understandable systems language
  - Relate categories together to work as a functioning system and lay it out as a working system analogy to make it more workable as an enterprise architecture design pattern.
  - Proposed PHIN Document Structure:
    - **Data Entry**
      - » Manual Data Entry for Events
      - » Electronic Data Entry for Events (add)
    - **Data Sharing / Data Exchange**
      - » Sharing Data between Public Health Partners
      - » Electronic Data Alerts from Clinical Systems
      - » Electronic Data from LIMS
      - » Data Messaging between Public Health Partners

    - **Data Management**
      Case Management
      Public Health Directory
    - **Data Analysis**
      Data Analysis & Visualization
    - **Infrastructure / Security**
      IT Security & Infrastructure

Recommendations
Summary

- **Develop implementation guidelines and promote AD maturity through standard processes:**
  - To enable distributed AD at the CDC to PHIN standards, CDC must provide systems engineering guidance and tools to the development organizations
  - Provide AD tools, guidance and shared code to help developers
  - Adhere to the SEI CMM for application development
  - Conduct AD reviews and perform self certification processes as part of the EA (e.g., internal team reviews, completion of compliance matrices, independent testing, etc.)
  - Participate fully in the EA governance processes.
- **Some specifics on the technical standards:**
  - PH partners need more specifics on the implementation and use of the public health directory component of PHIN (it is not granular enough to really tell who people are and what they can do yet)
  - PH partners need examples of working modules that demonstrate the PHIN's target architecture and how it works together
  - Allow industry to drive the more "leading" architectural components to specific standards (e.g., ebXML and HL7 v3.0).

Recommendations
Summary

- **How to make this work:**
  - Attach the PHIN standards to the money (i.e., cooperative agreements) like was done with the bioterrorism agreement.
  - The individual states will need to develop the required skills for each of these technologies - continue technical support from CDC is welcome by way of guidance and tools
  - Support and funding for developed applications from internal state leadership is critical
  - Consider outsourcing options to get states up and running on newer technologies, then transition application support to state teams with appropriate knowledge transfer
  - Security will continue to be difficult because it is required at all levels of state PH infrastructure and its not there now; CDC/PHIN should provide “transitional” guidance for these situations and independent verification & validation (IV&V) services to assist the states with security compliance.
  - Overcome the predisposition to build when buy is an option within PH community (communication, evaluations at CDC, etc.)
  - CDC to release several workable components, built to PHIN specs, to show the PH community how to interface, build basic components, etc. In particular - HL7 v3.0 and ebXML.
  - Emphasize the benefits to the PH partners in the states:
    - The feedback on the data that is sent to CDC, analyzed and then available for review
    - The potential to use clinical data for event detection
    - Analysis and visualization of data
    - Improved data collection and reporting process, timeliness and accuracy.

Conclusions

- **Conclusions:**
  - An independent review of the PHIN Version 1 has been completed
  - PH partners universally agree to the vision and overall direction of the PHIN
  - The PHIN standards and specifications are a strong start and are appropriate for use in PH, as annotated in this report
  - Success of the PHIN relies on both CDC and its PH partners—all must commit to this initiative in order for it to succeed
  - As the PHIN evolves, there are several gaps to be filled in the overall architecture
  - There are several enterprise architecture best practices to be employed that will help the CDC and its partners evolve the PHIN.

Q & A

Appendices

- Interviewees
- Industry Best Practice
  - Gartner's Enterprise Architecture Framework
  - Enterprise Architecture Governance
  - Enterprise Architecture Core Processes
  - Architectural Engagement Process
  - Business Continuity Planning
  - Technology Issues

Interviewees

Public Health Partners:

- Igor Soljan, Kent County Health Department, Michigan
- Larry Hanrahan, CSTE, Wisconsin
- Mike Perry, ATSDR CTO
- John Fitzpatrick, ATSDR
- John Tranetzki, Milwaukee Dept of Health
- Mike Davisson, ASTHO, NY Dept of Health
- Denton Peterson, NAPHIT

Internal CDC:

- David Fleming, CDC OD, Deputy Director for Public Health Science
- Jim Seligman, CDC CIO
- John Loonsk, CDC IRMO
- Laura Conn, CDC IRMO
- John Teeter, CDC IRMO
- Meade Morgan, CDC Global AIDS Prgm
- Bob Pinner, CDC NCID
- Dale Nordenberg, CDC NCID CIO
- Jeanne Gilliland, NCCDPHP
- Mike Koss, NCCDPHP
- Wayne Giles, NCCDPHP
- Joe Rogers, NCCDPHP
- Ken Gerlach, NCCDPHP

Industry Best Practice

Industry Best Practice

- **Gartner's Enterprise Architecture Framework**
- **Enterprise Architecture Governance**
- **Enterprise Architecture Core Processes**
- **Architectural Engagement Process**
- **Business Continuity Planning**
- **Technology Issues:**
  - Transport Services (e.g., ebXML/SOAP)
  - Directory Services (e.g., LDAP)
  - HL7 Messaging
  - Controlled Medical Vocabularies (e.g., LOINC, SNOMED)
  - Enterprise Nervous Systems

Gartner's Enterprise Architecture Framework

New Concepts and Tools for Actionable Results

Enterprise Architecture (EA)
Vision Statement (Sample)

The Enterprise Architecture (EA) will enable efficient business processes and information access for all CDC centers (i.e., “business units”) and trading partners by providing the necessary:

- Common models
- Frameworks
- Standards

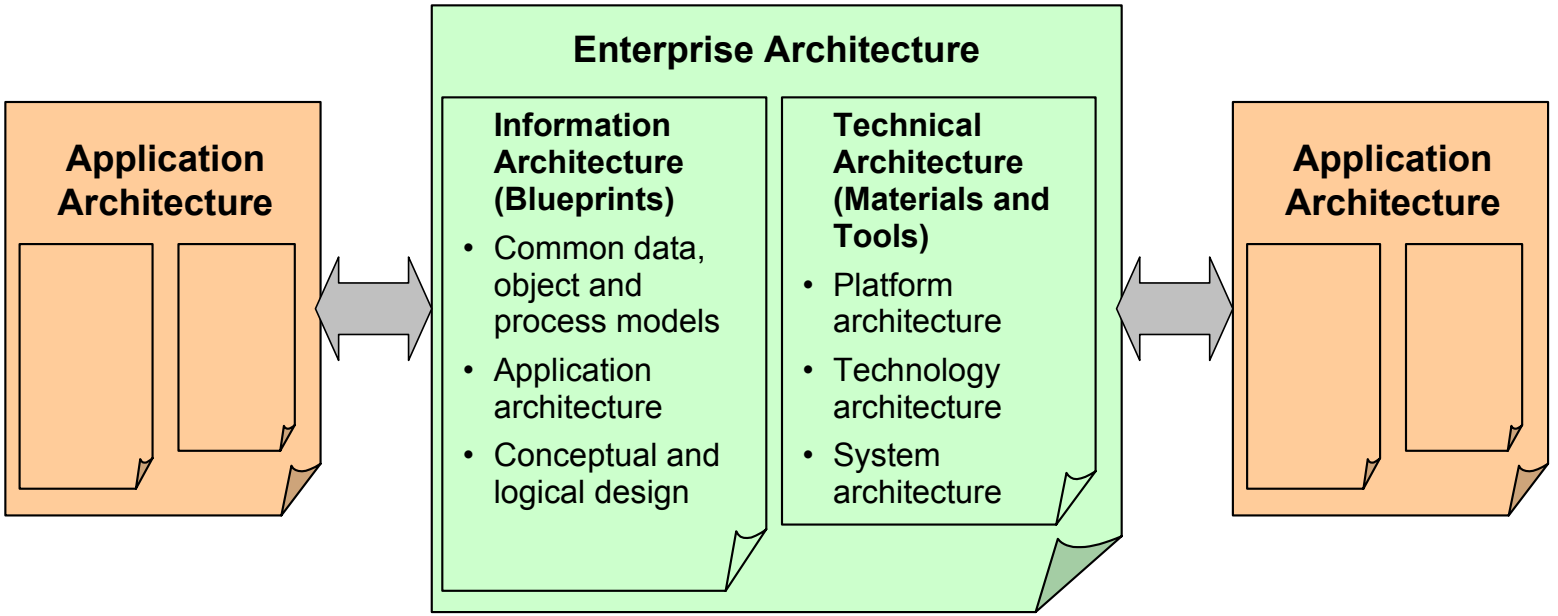
by which to build:

- Shared CDC enterprise systems
- Shared CDC/partner integration standards
- A secure and robust core IT infrastructure.

Definition of “EA”

A “blueprint” for implementing CDC and trading partner information systems to enable the mission: It is embodied in a set of policies, principles, models, design patterns and standards that guide development and integration of enterprise IT systems.

Enterprise IT systems and components are those that serve common needs across CDC centers (i.e., “business units”) and trading partners and that support CDC’s primary mission.



What is "Information Technology Architecture"?

Gartner View

IT Architecture Definitions

Short Form:

A framework and set of guidelines to build new information systems.

Long Form:

IT architecture is a series of principles, guidelines and design patterns used by an organization to direct the process of acquiring, building, modifying and interfacing IT resources throughout the organization. These resources can include equipment, software, interface protocols, communications, development methodologies, modeling tools, organizational structures and more.

IT is a new discipline; therefore, we have to use analogies and borrow terms from other fields.

If two different architects designed houses for two different sites, we would not expect them to be the same. They *would* have much in common, and we would certainly recognize that each was a house.

Just as an architect designs a house, an IT project architect relies on known design patterns, common materials, guidelines and sometimes even a "building code" (formal standards).

When Someone Says "Architecture"
What Does They Mean?

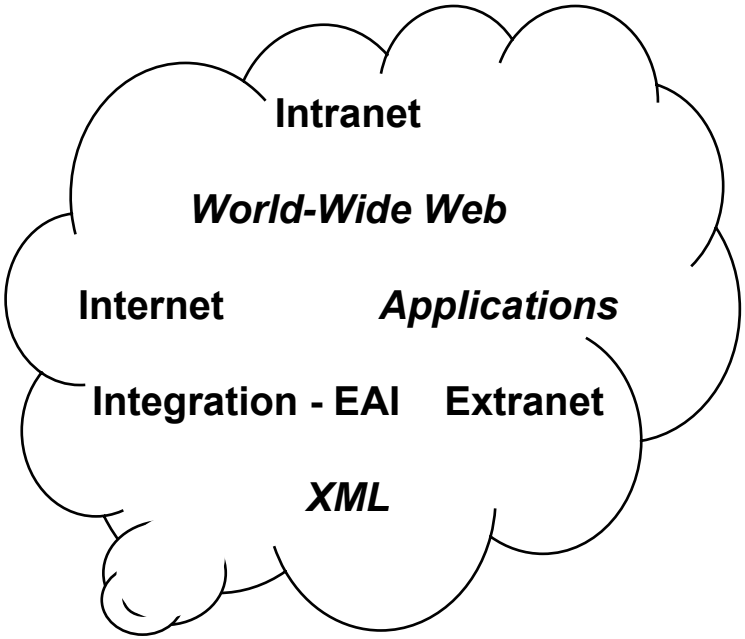
- **The term is not used the same way everywhere. It may imply any of the following …**

1. Kinds of architecture:

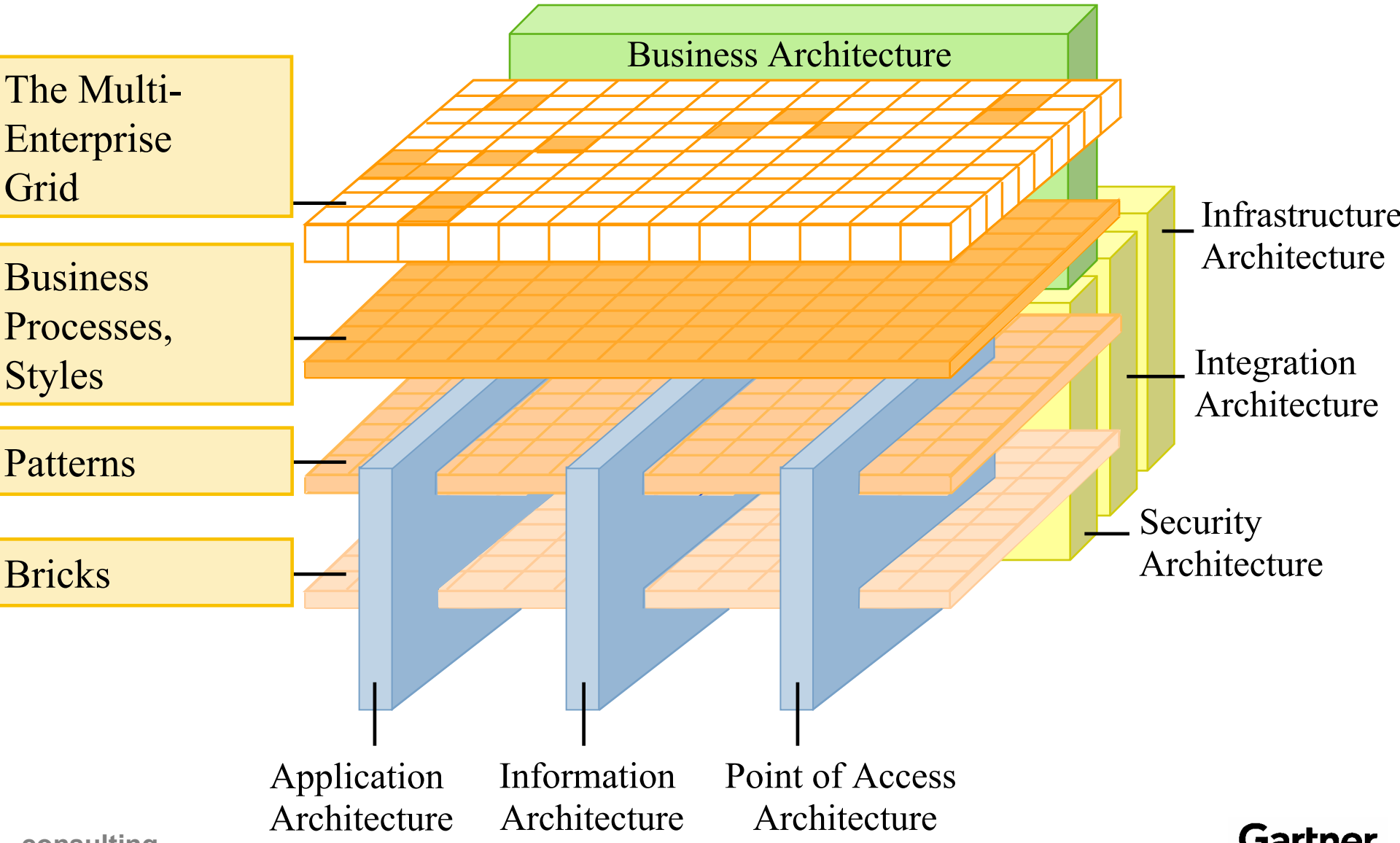
- application architecture
- network architecture
- middleware architecture
- object/component architecture
- **integration architecture**
- technical architecture
- **web (Internet / Intranet) architecture**
- **e-business architecture (B2C & B2B)**

2. Scope:

- project
- **enterprise**
- consortium
- etc.

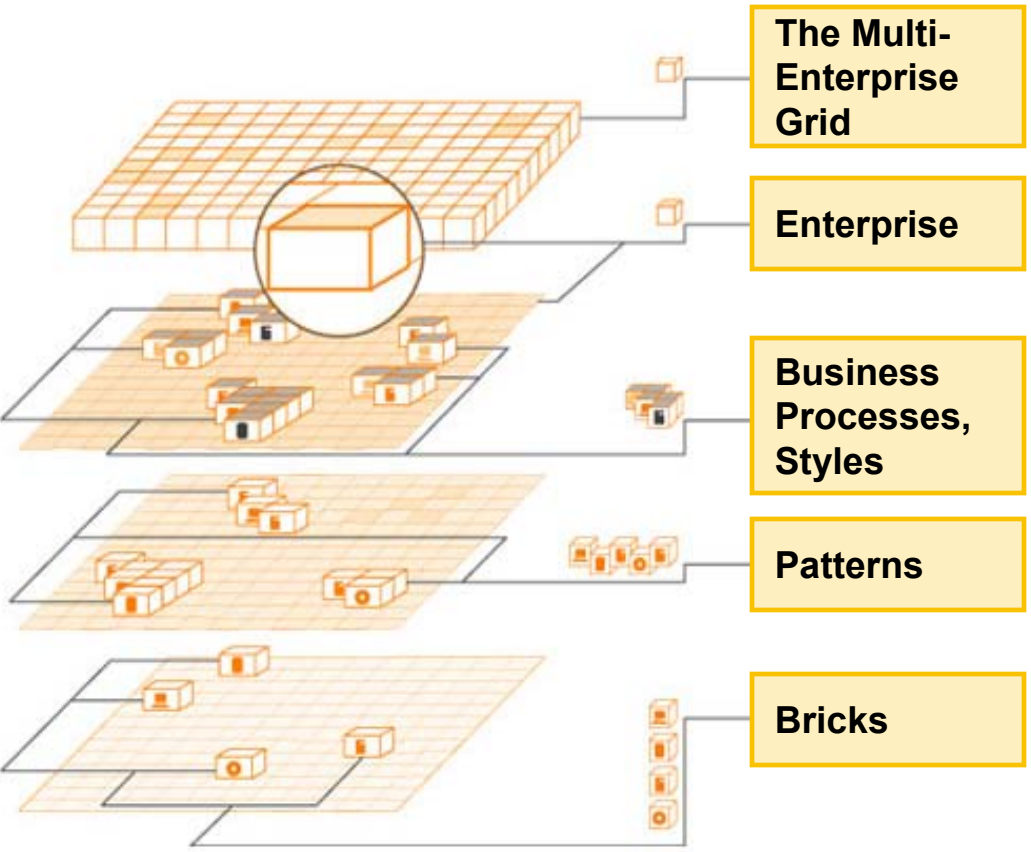


Gartner's Architecture Framework



Gartner's Architecture Framework

Gartner's approach to Architecture begins with a conceptual framework that includes Grids, Styles, Patterns and Bricks. The Grid is a logical framework that establishes the universe of discourse including the definition of the enterprise, the virtual enterprise, the applications universe, the network and other necessary common understandings.

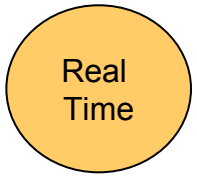
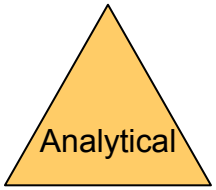


Styles are modes of processing such as transaction processing (OLTP), real-time, collaborative, analytical, and utility processing. Styles include the business activities, not just technology.

Next, Gartner's framework includes design patterns -- architectural models that show a logical view of the technology implementation of the the Styles.

At the lowest level are the elemental "bricks", fundamental building blocks, which are organized according to a formal taxonomy in the Technical Reference Model.

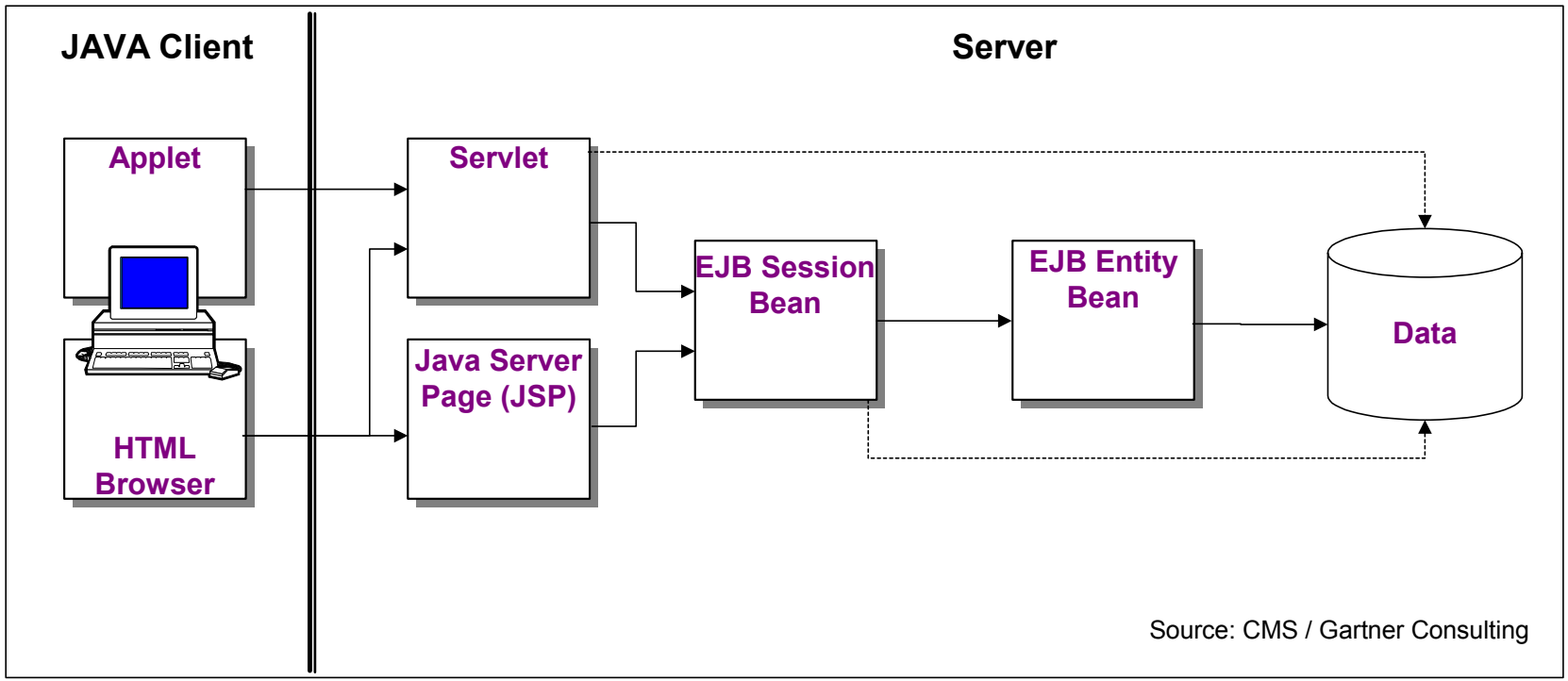
Business Process Styles Drive IT Architectural Styles

Business Process Style					
Computational Need	• Fail Safe • Priority Interrupts • 7 x 24	• Quick Response • Positive Commit	• Processing Intensive • Non-critical • Little or no programming	• Complex Indexing • Content Management • Messaging Choices	• Routine applications • Stability • Economy & dependability
Architectural Style	• Fault Tolerant • Queued Messages	• Multiple input modes • Transaction monitor • Web-based input	• Analytical packages • Data mart or warehouse	• Metadata tags • High bandwidth • Unstructured data	• COTS • Cost-driven • Outsource candidates

Logical Design Patterns

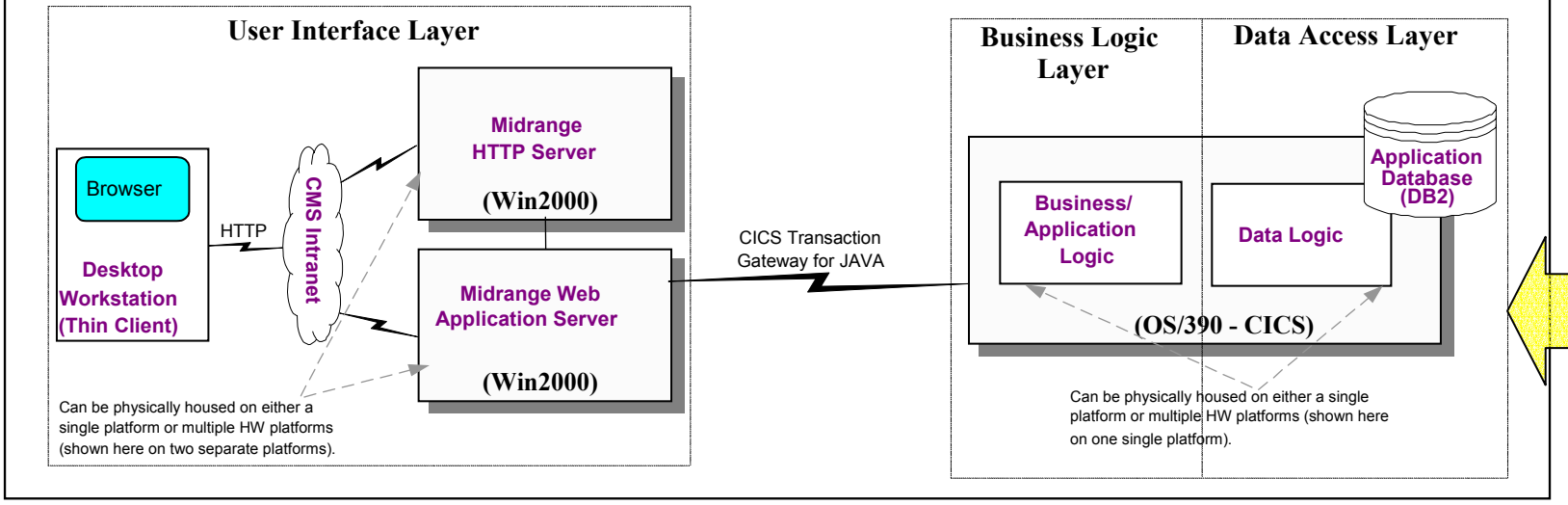
Design patterns are important in software architecture, network architecture (e.g., “partial mesh” topologies), security (e.g., “defense in depth”) and elsewhere.

Logical design patterns are included in the designer view. Physical design patterns that implement the logical design patterns are cataloged in the builder view.



Physical Patterns and Standard Configurations

EXAMPLE: Three-tier Transaction Processing pattern



Platform: Desktop Workstation (Thin Client)		
Major Service Area: Information Processing		
Processor	Desktop Workstation	Intel Compatible
Operating System	Desktop Workstation OS	Windows 2000
Major Service Area: Applications		
Standard Office Productivity Tools	Web Browser	MS Internet Explorer

Platform: Midrange HTTP Server		
Major Service Area: Information Processing		
Processor	Midrange Server	Intel Compatible
Operating System	Server OS	Windows 2000 Advanced Server
Enabling SW	HTTP Server	Apache

Platform: Midrange Application Server		
Major Service Area: Information Processing		
Processor	Midrange Server	Intel Compatible
Operating System	Server OS	Windows 2000 Advanced Server
	Security	Login to MS Network
	Security	RACF
	User Interface	Java Server Pages
Major Service Area: Middleware		
Transaction Services	Web Application Server	WebSphere Application Server
	Enterprise Transaction Server Client	CICS Transaction Gateway

Platform: Enterprise Application Server		
Major Service Area: Information Processing		
Processor	Enterprise Server	S/390 Mainframe
Operating System	Server OS	OS/390
	Security	RACF
Major Service Area: Middleware		
Transaction Services	Enterprise Transaction Server	CICS Transaction Server
Major Service Area: Data Management		
Structured Data Management	RDBMS Data Storage	DB2

Source; CMS / Gartner Consulting

Standard platform configurations that implement the pattern

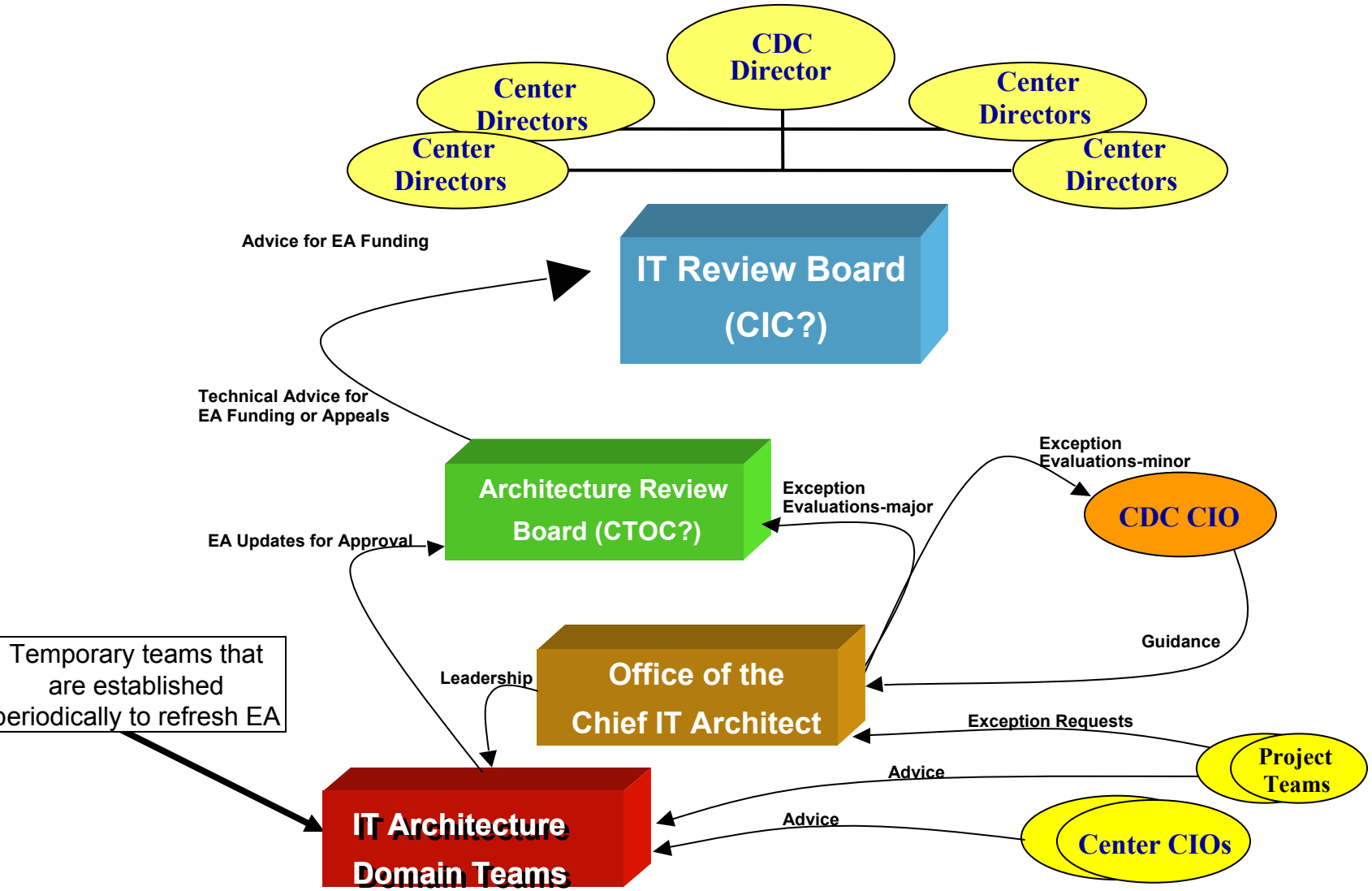
Enterprise Architecture Governance

EA Participants and Governance

Body	Members	Decisions
IT Review Board	Executives	Role of IT, Direction, Spending
Architecture Review Board (ARB)	CIO, Business Unit CIOs, Enterprise App Architects	Arch. Direction, Approval, Exceptions
Office of Chief IT Architect	Chief Architect, Enterprise Architects	Benefits, Direction, Adherence
IT Architecture Domain Teams	Enterprise Architects, SMEs	Renewal of Architecture (by Domain)

EA Governance Structure

CDC Example based on work for the NIH



Roles and Responsibilities

CDC Example based on work for the NIH (Continued)

Organization	Description	Roles and Responsibilities	Involved How?
IT Architecture Domain Teams	■ Teams with 6 to 12 members with representation across the centers ■ Subject matter experts from IT ■ Subject matter experts from functional organizations for relevant domains (e.g., Applications and Data) ■ Each Team has a defined architectural focus (e.g., application integration, network infrastructure)	■ Update the EA on a revolving basis. (e.g., at least 1/3 per year) ■ Represent interest and requirements of the centers ■ Consider changes in CDC mission drivers ■ Conduct reviews of current state ■ Determine technology options ■ Evaluate, make recommendations regarding products, methodologies, industry standards ■ Link choices back to the CDC mission and strategy to the extent possible ■ Etc.	■ Core Architecture Processes ■ Majority vote carries
Office of the Chief IT Architect	■ Full Time IT Architecture Staff: ❑ Chief IT Architect ❑ Subject matter experts ❑ Administrative support	■ Lead renewal of architecture and standards ■ Lead and facilitate Domain Team activities ■ Ensure CDC mission and architecture alignment ■ Lead assessment of evolving technologies for standards adoption or renewal ■ Develop recommendations for the "Architecture Review Board" as the basis for decision-making ■ Represent CDC Architecture to HHS ■ Etc.	■ Core architecture processes ■ Business and IT planning ■ Project life cycle process

Roles and Responsibilities

CDC Example based on work for the NIH (Continued)

Organization	Description	Roles and Responsibilities	Involved How?
CDC CIO	■ Sponsor and advocate of the EA	■ Promotes understanding and buy-in of EA benefits ■ Chairs the Architecture Review Board ■ Provides guidance to the Office of the Chief IT Architect ■ Rules on minor exception requests from project teams, considering recommendations from the Chief IT Architect	■ Uses core architecture processes ■ Educates and persuades peer and superior executives in other forums
Center CIOs & IT Staff	■ Center CIOs and their respective IT staffs	■ Active participation in the Architecture Review Board and membership in Domain Teams. ■ Review and comment on Domain Team recommendations ■ Contribute "showcase implementations" and architecture related best practices ■ Foster adherence to the portions of EA in scope for their organizations	■ Board membership ■ SME participation in domain teams ■ Use core architecture processes

Roles and Responsibilities

CDC Example based on work for the NIH (Continued)

Organization	Description	Roles and Responsibilities	Involved How?
Architecture Review Board	■ 10 executive-level members: Center CIOs, Enterprise App Program Mgrs, CDC CIO ■ Generally meets quarterly and on special requests/ needs.	■ Initially, a forum to gain agreement: ❑ Enterprise architecture will benefits ❑ The level of effort involved (including Center staff [IT and non-IT]) ❑ Commitment to comply with the guidelines. ■ Ongoing responsibilities include: ❑ Monitoring the state of the architecture program and compliance ❑ Adjudicate serious architecture related conflicts ❑ Establishing working groups as necessary	■ Regular Meetings ■ Uses core architecture processes ■ Majority vote carries
IT Review Board	■ Executives from Centers	■ Approve architectural recommendations requiring investment ■ Support, endorse the EA ■ Rule on issues appealed from the Architecture Review Board	■ Regular budget process ■ Special meetings to consider architectural investments or appeals

EA Core Processes

Architecture Refresh

Standards

Project Review for Adherence

Exception Handling

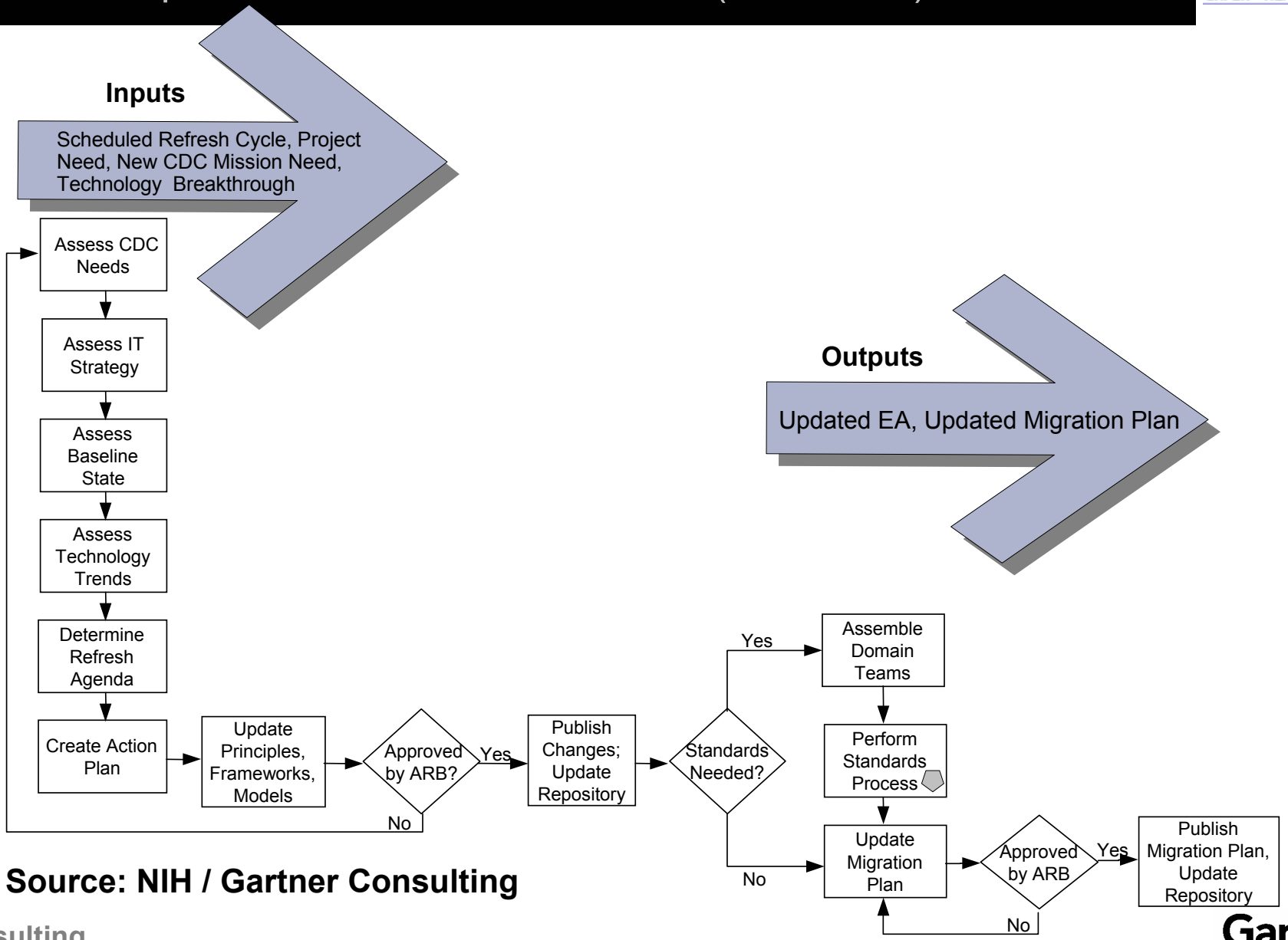
Architecture Refresh Process

CDC Example based on work for the NIH (Continued)

- **The process by which the EA and standards are refreshed—based on new technologies, business strategy changes, CDC center needs, or project team and center best practices**
  - Review changes to CDC mission or strategy
  - Review CDC IT strategy
  - Evaluate technology trends
  - Evaluate the current EA and its alignment to changing business needs, mission, and drivers
  - Plan the Refresh Agenda
  - Update principles, frameworks, models and seek ARB approval
  - Activate IT Architecture Domain teams and execute the Standards Process
    - Bring in additional Subject Matter Experts as required
    - Solicit input of IT project teams and IT staff (cross-center) as required
  - Publish the approved EA
  - Create / update EA migration plan
  - Seek ARB approval of the EA migration plan
  - Publish the approved EA migration plan

Architecture Refresh Process Flow

CDC Example based on work for the NIH (Continued)



Source: NIH / Gartner Consulting

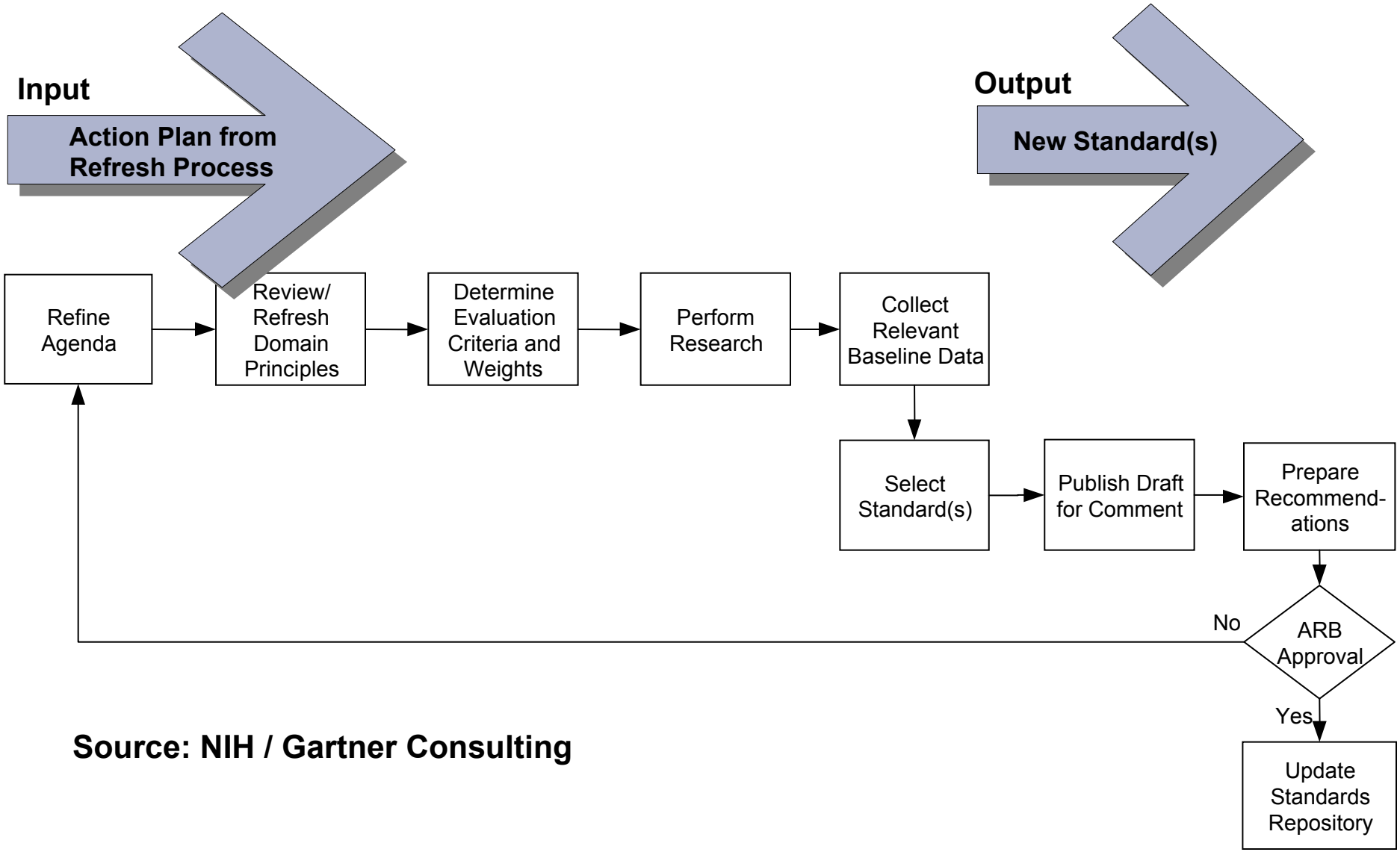
Standards Process

CDC Example based on work for the NIH (Continued)

- **The process used by IT Architecture Domain Teams by which the standards are updated:**
  - Refine agenda for the domain
  - Review/revise domain principles
    - To guide decision making and creation of selection criteria
  - Develop Standards Selection Criteria
    - Must include criteria relevant to the CDC's Mission and needs of the centers
    - Must include weights for the criteria
  - Perform Research
    - Consult objective outside sources
  - Develop/select standards (technology, product, and process standards as appropriate)
  - Draft selected standards and publish for comment
  - Create final recommendations
  - Seek ARB approval of standards and models (revise as necessary)
  - Publish and update the standards repository

Standards Process Flow

CDC Example based on work for the NIH (Continued)

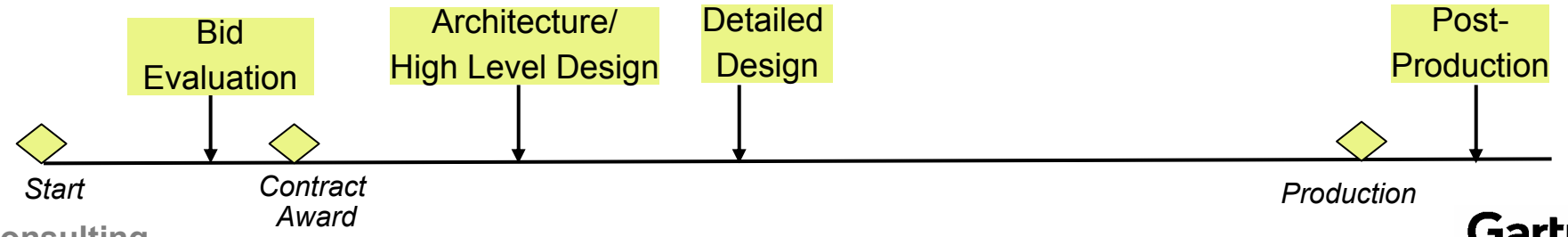


Source: NIH / Gartner Consulting

Project Review for Adherence Process

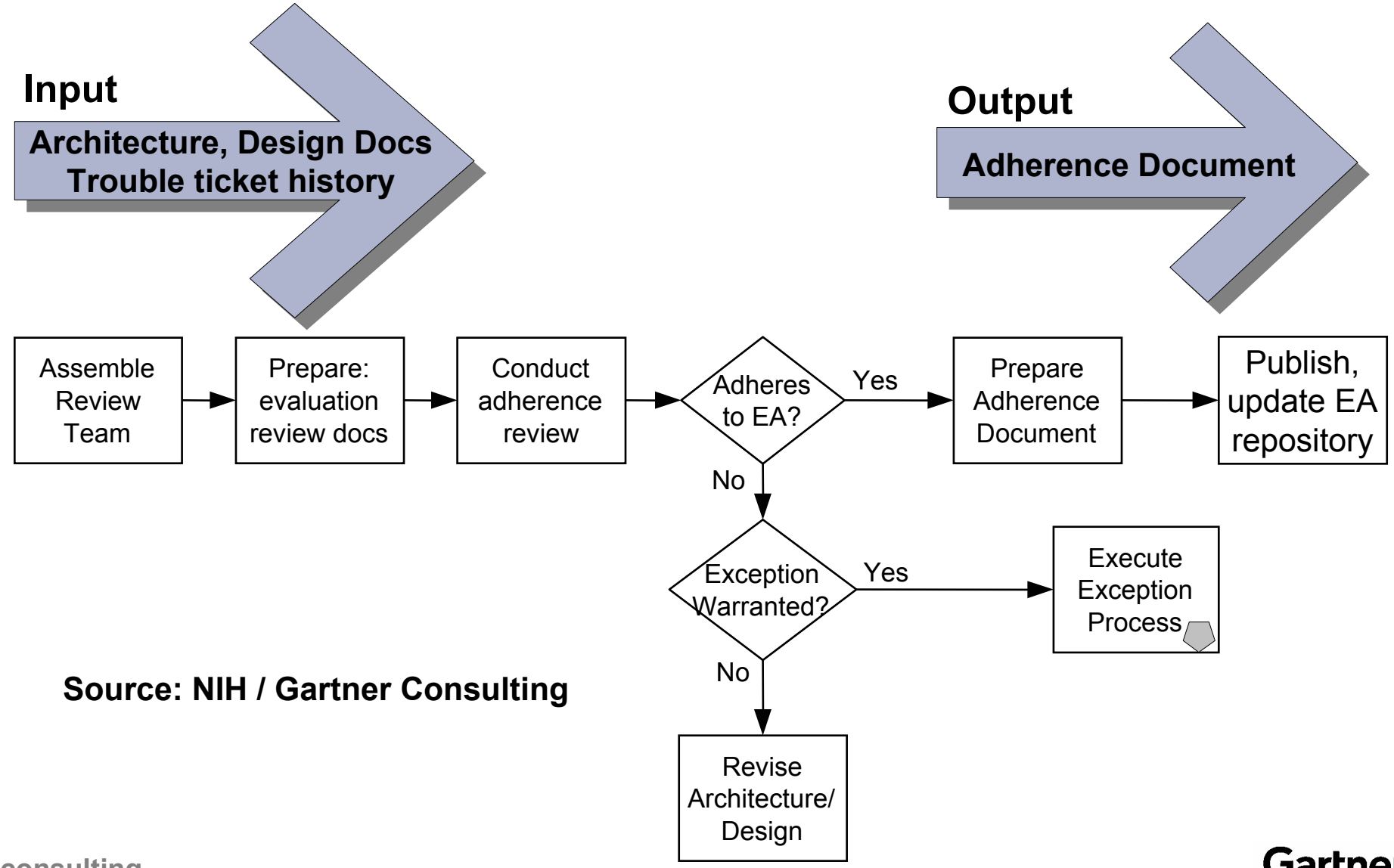
CDC Example based on work for the NIH (Continued)

- **The process by which projects are evaluated for adherence to the enterprise architecture:**
  - The general approach is self-certification
    - Each Project Steering Committee leads self certification of its project, requesting assistance from the Chief IT Architect when necessary
    - Contractors self certify compliance to the EA (e.g., compliance work with eHARS and NEDSS)
    - Architects of the Office of the Chief IT Architect will attend if project has significant EA impact
  - Self certification occurs at several points in the life cycle:
    - When bids are submitted by contractors
    - First architecture/high level design review
    - Detailed design review
    - Post production review (as built)
      - This is the opportunity to provide feedback to the Office of the Chief IT Architect: What worked? What didn't? Changes warranted?
  - Results are published in the EA repository



Project Review for Adherence Process Flow

CDC Example based on work for the NIH (Continued)



Source: NIH / Gartner Consulting

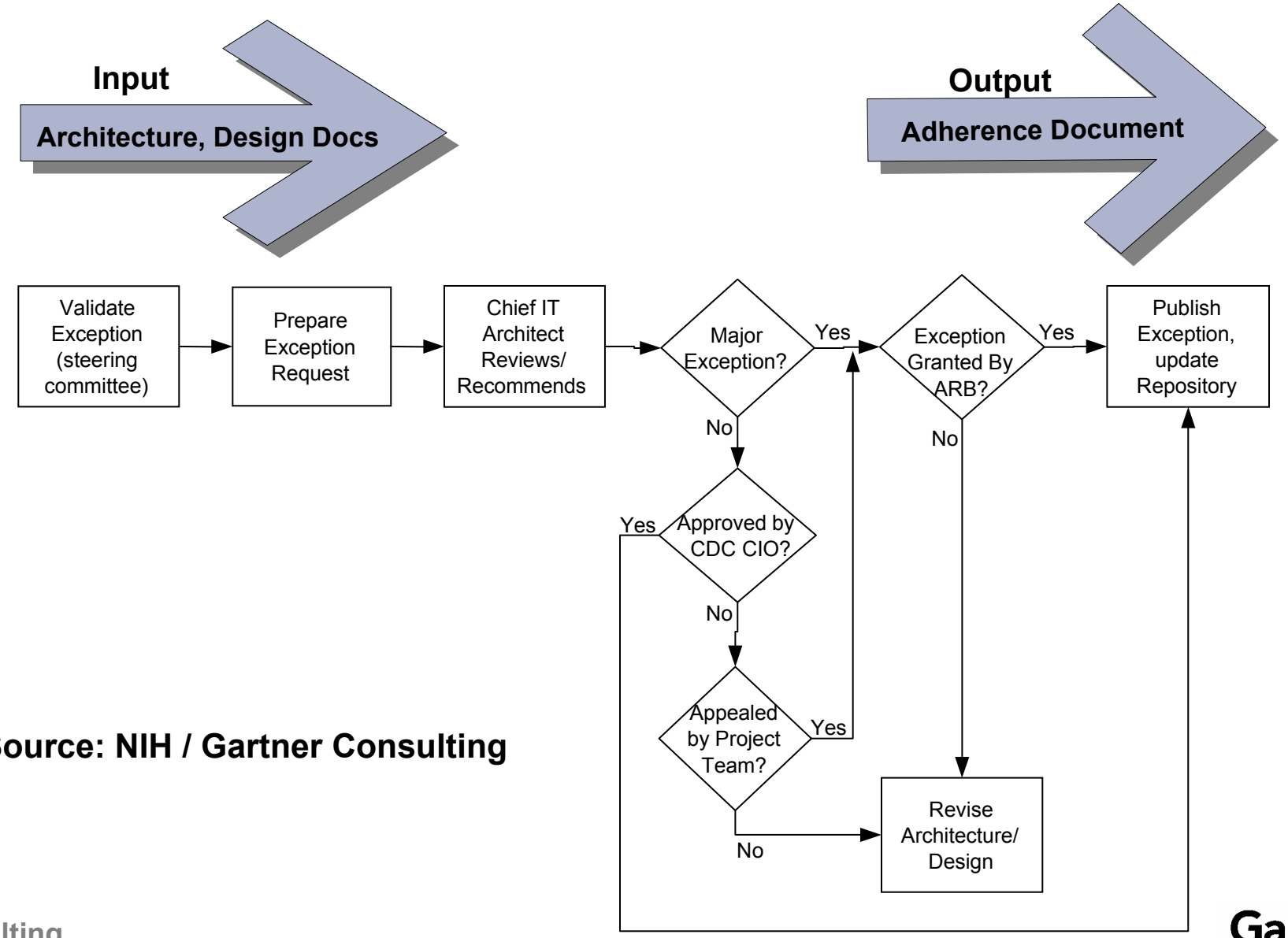
Exception Handling Process

CDC Example based on work for the NIH (Continued)

- **The process for evaluating and granting waivers to following the enterprise architecture**
  - Project team submits exception request to Office of Chief Architect
    - Other parties may submit exception requests; however, it is anticipated that the need will generally arise due to a planned project
    - Valid reasons include:
      - New technology needed that is not currently defined in the EA
      - Project would benefit from a technology in the EA labeled as “emerging”
      - External partner is driving a required standard different from the NIH EA
      - Other mission-based need
    - Requests must include a business case and impact analysis
  - Chief IT Architect recommends action
  - NIH CIO approves minor exceptions
  - ARB approves major exceptions
  - Exceptions are published in the EA repository

Exception Handling Process Flow

CDC Example based on work for the NIH (Continued)



Source: NIH / Gartner Consulting

Architectural Engagement Process

Architectural Engagement Process
Architectural Benefits

- **It is important to promote the following benefits of the architecture to both the governance structure and to the application developers:**
  - Interoperability—fast, effective system and data integration across systems
  - Low support costs—fewer disparate technologies to purchase, learn and support
  - Faster design—Faster accommodation of new requirements
  - Simpler system management—fewer component parts and measures
  - Easier transferability of personnel
  - Clearer vision of strategic direction
  - Ability to adapt to changing business and technology requirements

Architectural Engagement Process
Stakeholder Roles in Architectural Compliance

	Stakeholder						
Task	**Executive Steering Committee**	**Project Office**	**CIO**	**Project Sponsor**	**Project Team**	**Full-Time Architects**	**Architecture Task Force**
Document Architecture Standards and Guidelines		T	O	T	C	MC	I
Document Self-Assessment Criteria		T	O		C	MCT	I
Plan Project		T or C	AI	O	MI	AC	
Approve Project	I or A	M	A	O			
Initiate Project		T or C	A	O	MI		
Design Project		T	T	O	MI	AC	
Implement Project		T	T	O	MI	C	
Complete Project	T	A	A	O	MI	A	
Negotiate Conflicts	A	M	I or A	O	I	I	
Monitor Compliance	T	M	O	T	T	I	

O=Own, M=Manage, A=Agree, I=Involve, C=Consult, T=Tell

Source: Gartner Research

Architectural Engagement Process
Architectural Compliance Tasks

- **Task 1. Document architecture standards and guidelines.** Architecture standards and guidelines must be published and available to projects so the project team can incorporate them into designs and plans.
- **Task 2. Document self-assessment criteria.** There are many projects that have minimal or no impact on architecture, as they work within previously approved frameworks. An example of such a criterion is that the project uses only technology that conforms to the architecture standards.
- **Task 3. Plan the project.** In this task, a project builds its business case, including the schedule and resourcing plan. To do this, there must be at least a high-level understanding of the solution. Architects should at least be involved in a consulting capacity to resolve possible architectural issues. For major projects, they should work with the project team to plan the proposed solution.
- **Task 4. Approve the project.** All projects, except those that conform to the self-assessment criteria, must undergo an architecture review.
- **Task 5. Initiate, design and implement the project.** When a project is being resourced, architects may be scheduled to work on designated design tasks that are required for project approval. Architects should also participate in quality assurance activities such as project design inspections and walk-throughs.
- **Task 6. Complete the project.** A final project review should be carried out by the project office to identify what was done well and to target areas for improvement.
- **Task 7. Negotiate conflicts.** From time to time, project teams and architects will be unable to agree on the solution design. A senior business body, such as an executive steering committee, must adjudicate deadlocks of this kind.
- **Task 8. Monitor compliance.** To complement architecture self-assessment, an audit program to monitor architectural compliance should be instituted. This program, conducted by the architects, should check whether the standards are being interpreted and applied correctly.

Architectural Engagement Process
Summary

The architecture engagement process must encompass a range of tasks, with a particular focus on solution design. Tasks to include are 1) document architecture standards and guidelines; 2) document self-assessment criteria; 3) plan the project; 4) approve the project; 5) initiate, design and implement the project; 6) complete the project; 7) negotiate conflicts; and 8) monitor compliance.

The architecture engagement process must provide ways of managing exceptions to architecture guidelines.

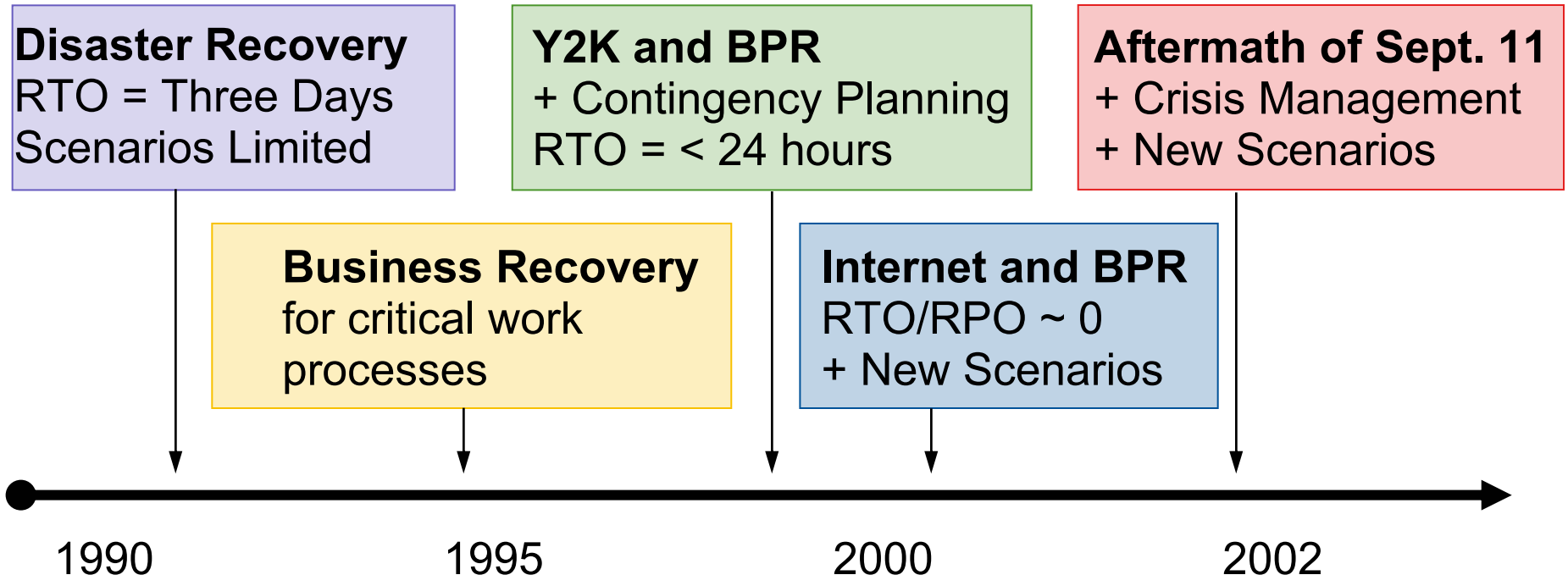
The engagement process should include feedback from projects so that the standards and guidelines are relevant, understandable and practical.

Bottom Line: Without an effective architecture engagement process, system architectures will not be put into practice. Instead, they will be ignored, rendering architecture objectives unachievable.

Business Continuity Planning

Evolution of Business Continuity

Sept. 11 Forever Changed Business Continuity Planning



BCP and DR (Cont'd)

Business Continuity Components

	Disaster Recovery	Business Recovery	Business Resumption	Contingency Planning
Objective	Mission-critical applications	Mission-critical business processing (workspace)	Business process workarounds	External event
Focus	Site or component outage (external)	Site outage (external)	Application outage (internal)	External behavior forcing change to internal
Deliverable	Disaster recovery plan	Business recovery plan	Alternate processing plan	Business contingency plan
Sample Event(s)	Fire at the data center; critical server failure	Electrical outage in the building	Credit authorization system down	Main supplier cannot ship due to its own problem
Sample Solution	Recovery site in a different location	Recovery site in a different power grid	Manual procedure	25% backup of vital products; backup supplier

Crisis Management

BCP and Disaster Recovery (*Cont'd*)

Project Life Cycle

Bus. Req.	System Arch.	System Design	Con-struct	Test	Imple-ment	Post Imple-ment
• Identify technology and ***business continuity*** risks from a business perspective - ***BIA/ Risk Analysis RTO/RPO*** • Ensure complete cost estimate • Ensure appro-priately protected end product	• Assess risks of new technology products • Identify security infrastructure reqs. • Identify sec. admin. reqs. • Establish security responsibilities and service-level regs. • ***Identify business continuity/DR strategies*** • Establish security test strategy	• Translate security architecture to detailed security infrastructure design • Develop security baselines for new technologies/ products • Develop detailed sec. admin. design • ***Develop detailed BCP/DR design/strategy*** • Develop draft SLAs • Develop security test plan	• Build/code security infrastructure env. and procs. • Build/code sec. admin. env ., roles/profiles and procs. • ***Build BCP/DR env., plans and procs.*** • Build/code security test plan, procs., scripts and test env.	• Train sec. admin., operations, business unit, etc. staff • Identify security non-compliance issues • Identify new security exposures • ***Test BCP/DR plans to ensure that RTO/RPO is attainable***	• Turn over secure application infrastructure to production • Implement sec. admin. roles/profiles • ***Implement business/ continuity DR env.***	• Identify changes to tested env. • Finalize sec. admin. env. and procs. • Finalize security infrastructure env. and procs. • ***Finalize BCP/DR env., plans and procs.*** • Assess SLA accuracy • Finalize risk acceptance with business • Ensure that info. sec. policies are current

BCP and Disaster Recovery (*Cont'd*)

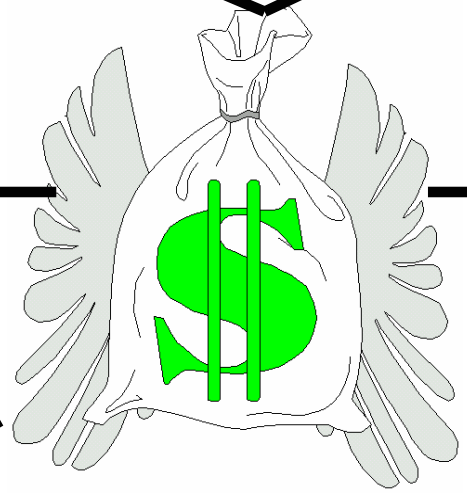
What is the "Cost of Downtime"

Productivity

- Number of employees impacted X hours out X burdened hourly rate

Revenue

- Direct loss
- Compensatory payments
- Lost future revenues
- Billing losses
- Investment losses



Damaged Reputation

- Customers
- Suppliers
- Financial markets
- Banks
- Business partners
- Etc.

Financial Performance

- Revenue recognition
- Cash flow
- Lost discounts (A/P)
- Payment guarantees

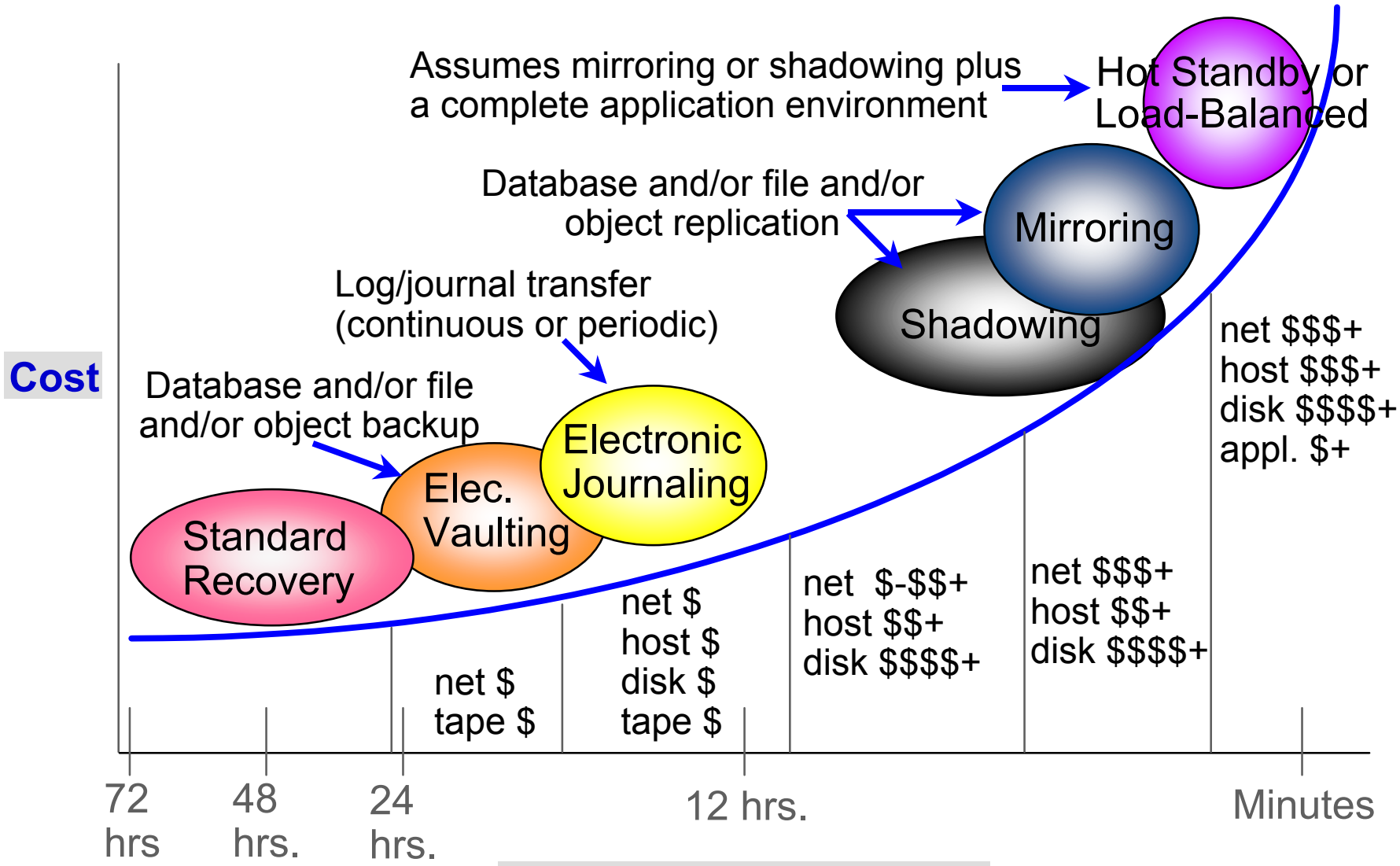
Know your downtime costs per hour, day, two days, etc.

Other Expenses

Temporary employees, equipment rental, overtime, extra shipping, travel expenses, etc.

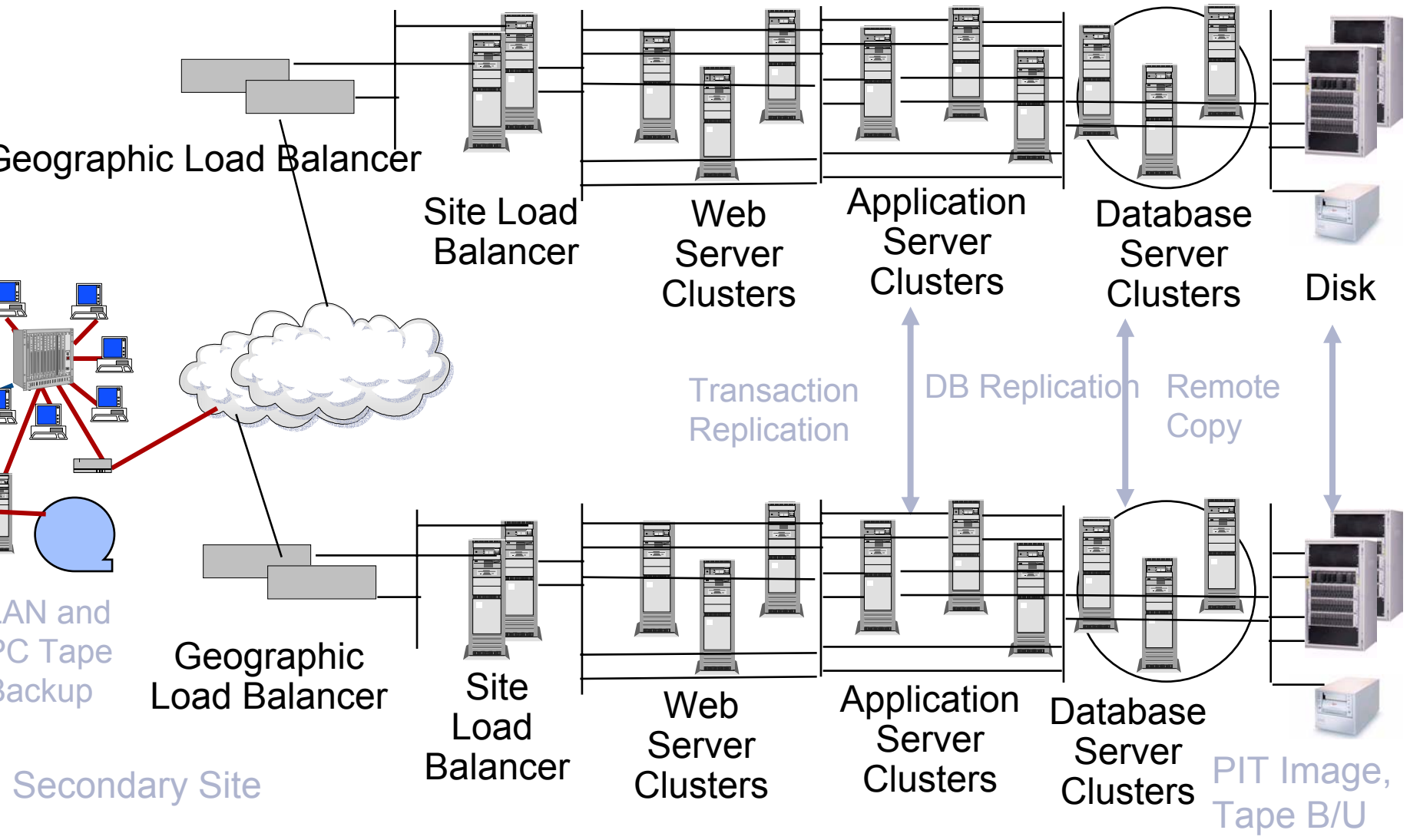
BCP and Disaster Recovery (*Cont'd*)

Applying High Availability to Disaster Recovery



BCP and Disaster Recovery (*Cont'd*)

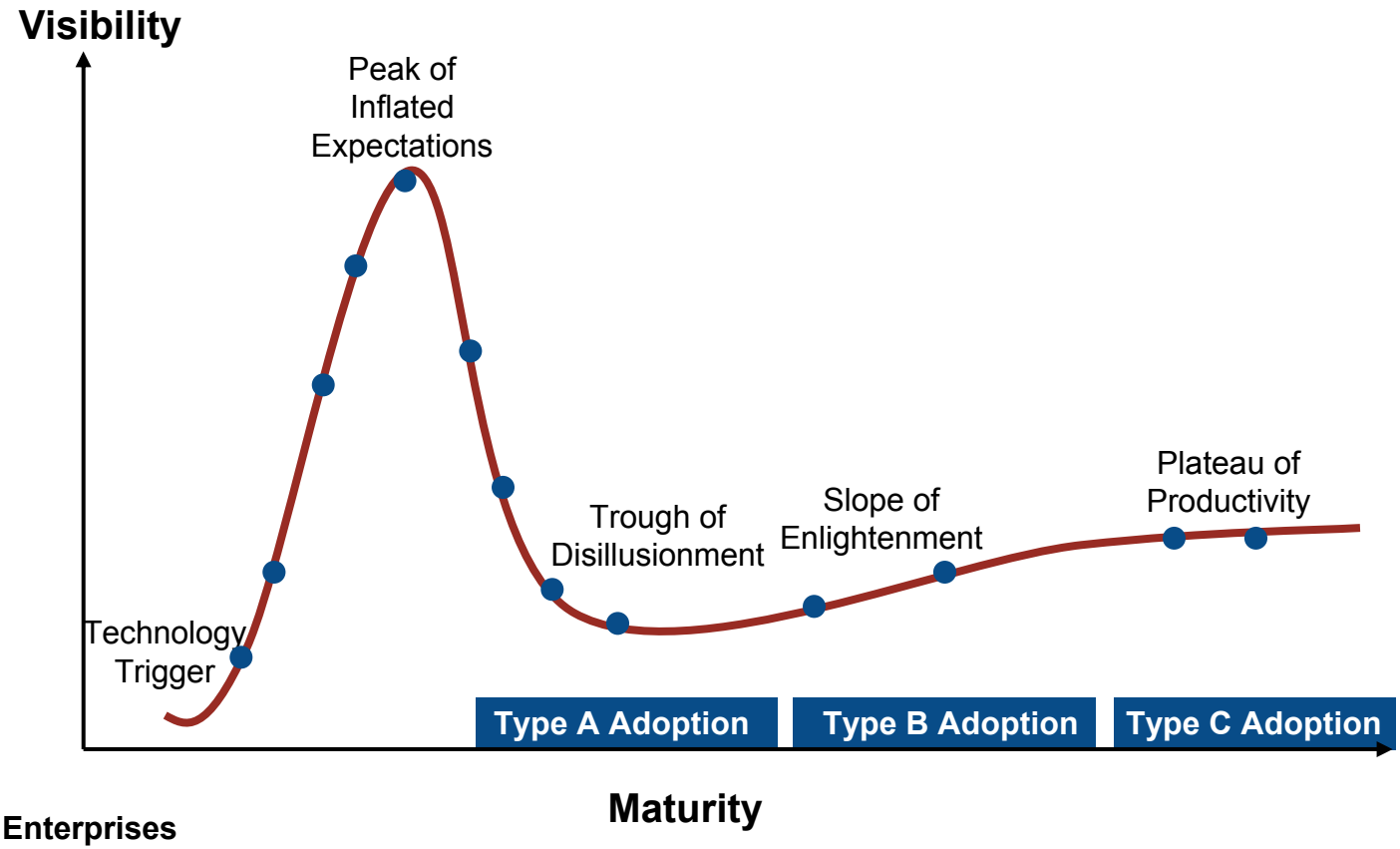
Disaster Recovery Architecture



Technology Standards

Gartner Technology Hype Cycle

The Hype Cycle Explained
Gartner's hype cycle is designed to help enterprises make intelligent decisions about when to implement emerging technologies. As is the case with all technology investments, there is no simple answer; rather, business needs, and philosophies, should determine when it makes sense to invest in a particular new technology

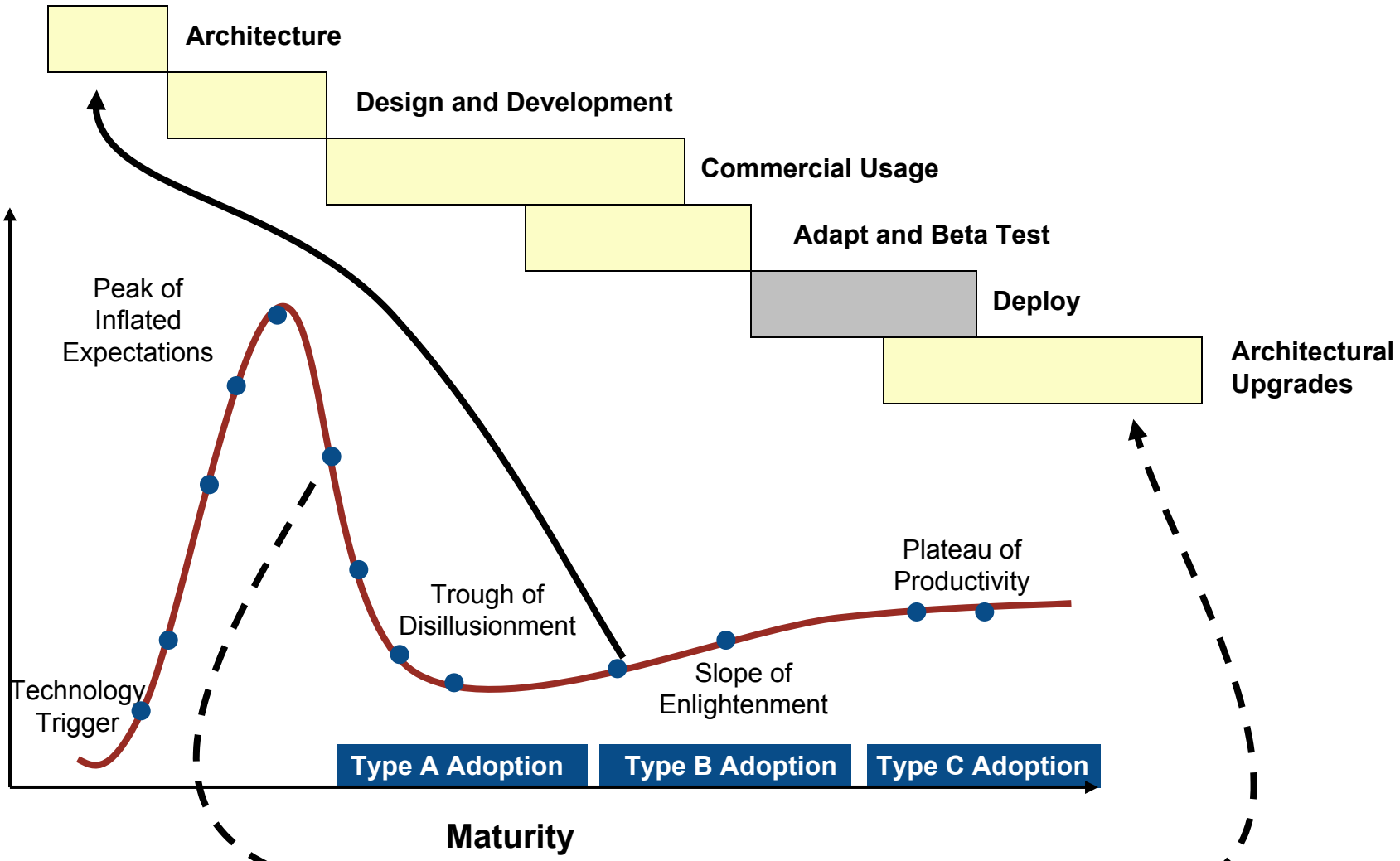


Type A, Type B and Type C Enterprises

Enterprises are identified as "Type A", "Type B" and "Type C", based on the aggressiveness with which they adopt and use technology (i.e., put an application into production):

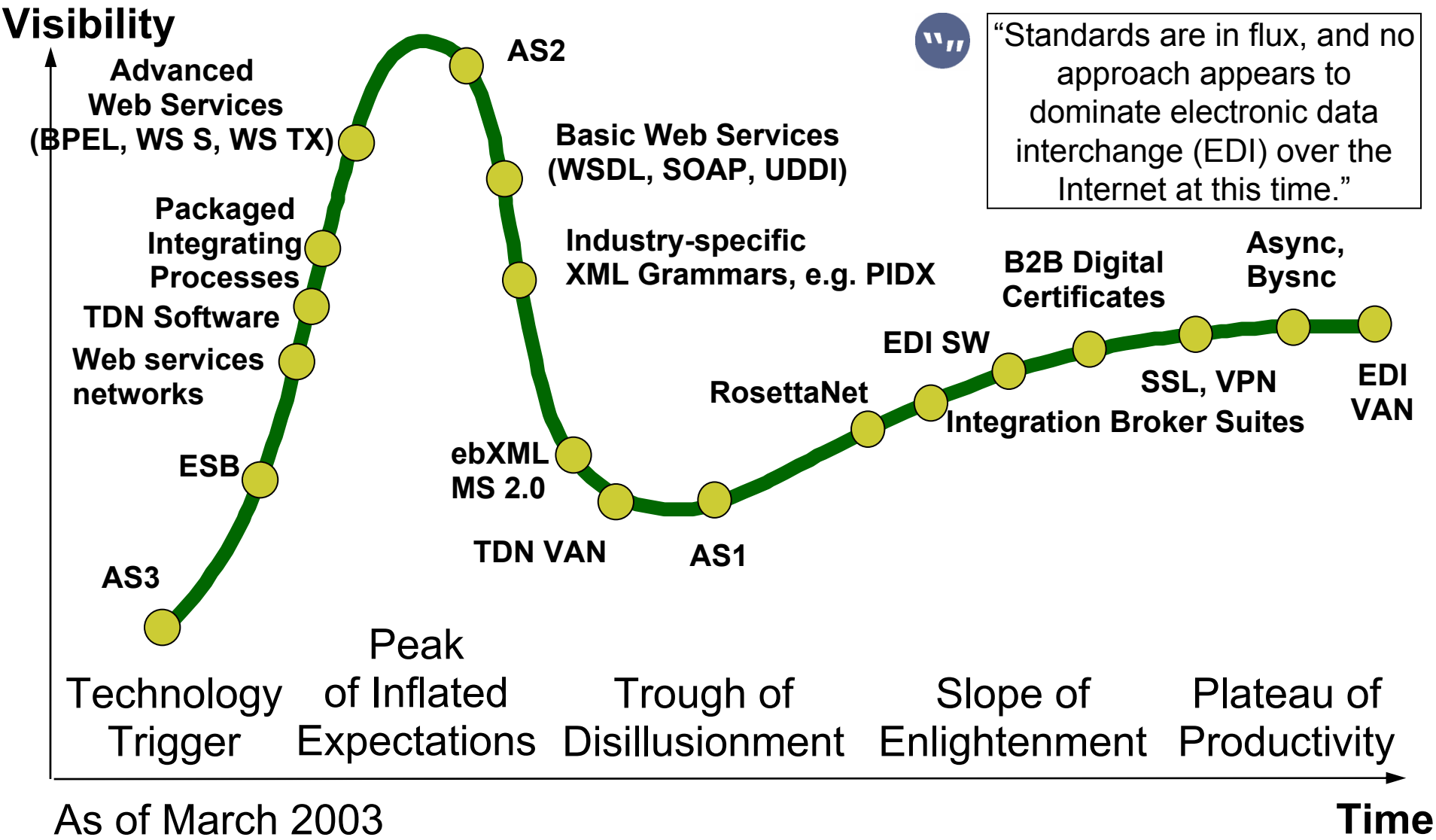
- Type A enterprises are technology-driven, often using immature, cutting-edge technologies to gain an edge.
- Type B enterprises are moderate technology adopters, implementing new technologies that have entered the mainstream.
- Type C enterprises are technologically risk-averse and are usually among the last to adopt new technologies.

Hype Cycle Position vs Deployment Decisions Using COTS Software



Transport Services

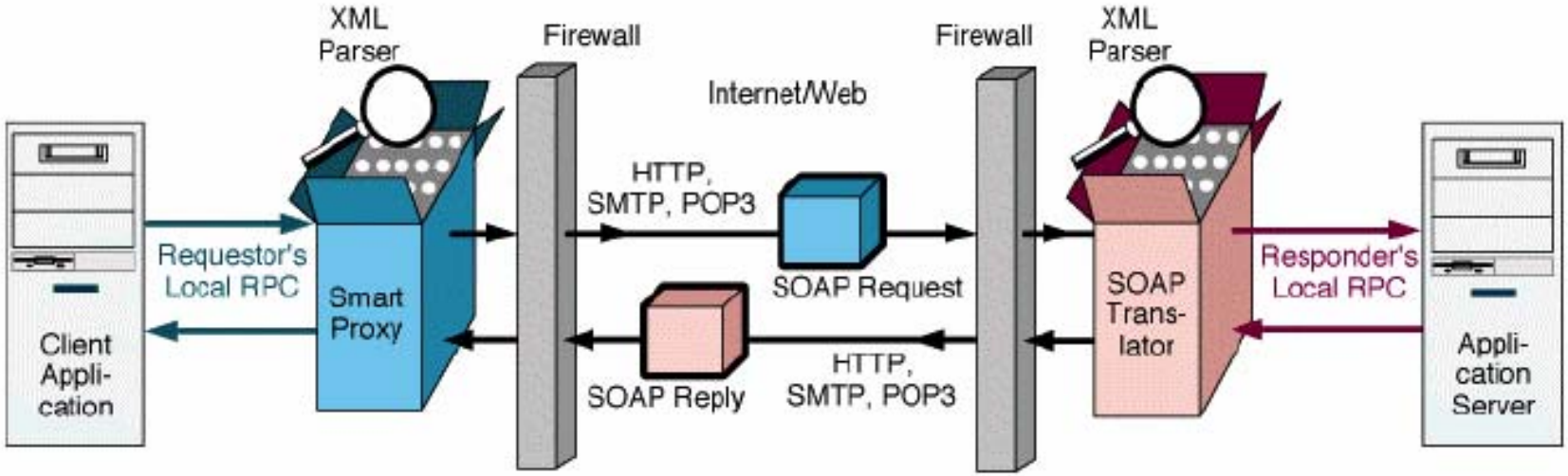
B2B Application Integration Technology Hype Cycle



"Standards are in flux, and no approach appears to dominate electronic data interchange (EDI) over the Internet at this time."

Transport Services
SOAP

SOAP lets one application invoke a remote procedure call (RPC) on another application or pass an object to a remote location using an XML message and the Internet. SOAP satisfies the growing need for business partners to exchange structured data over the Web independently of each other's underlying application platform. It is designed to let organizations publish data and services over the Web as easily as they can publish HTML pages. As such, it functions as a wire protocol to connect multiple Web portals, each of which might use an information server, object broker, or other facilities to integrate and process the information.



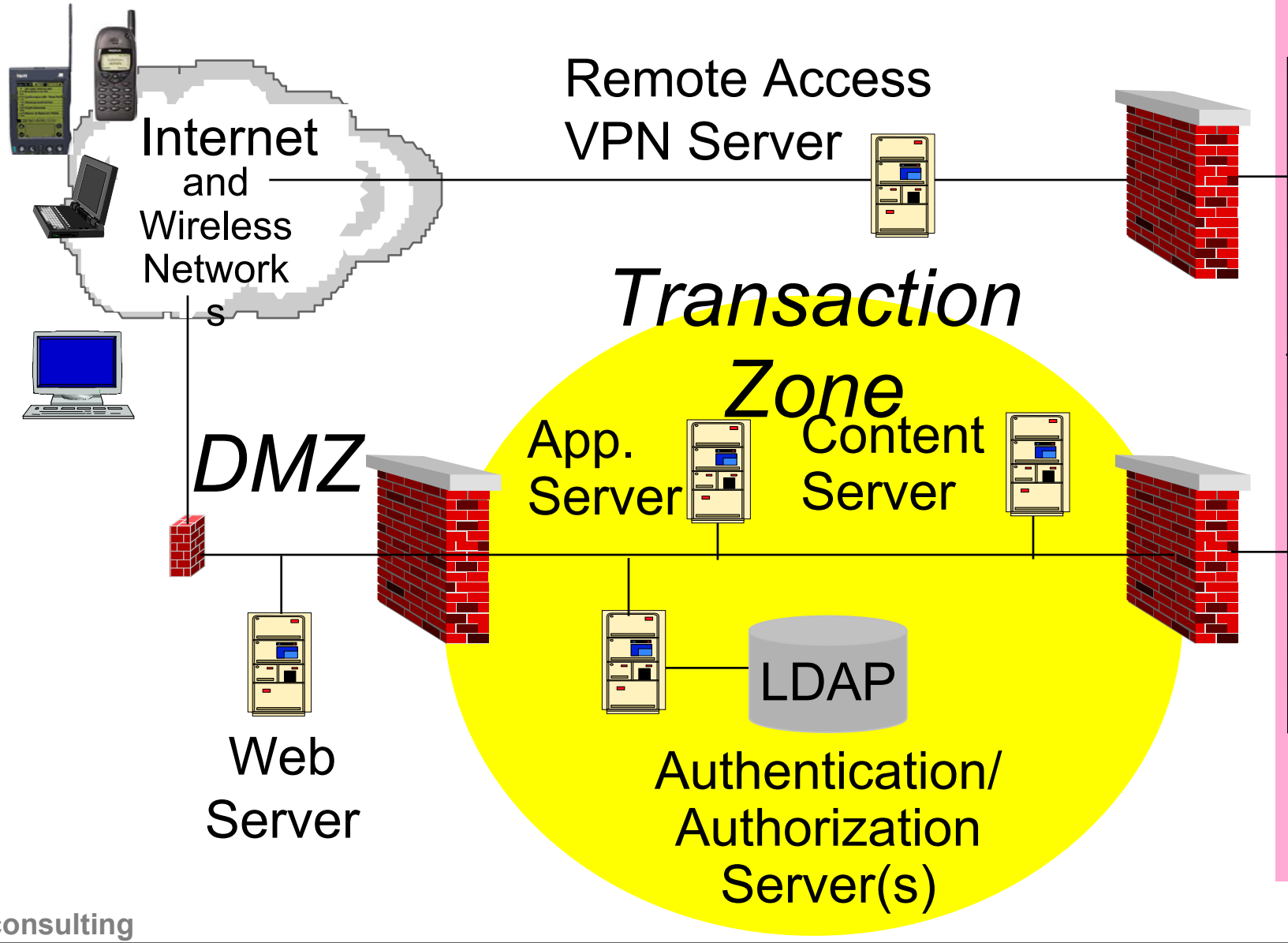
Transport Services

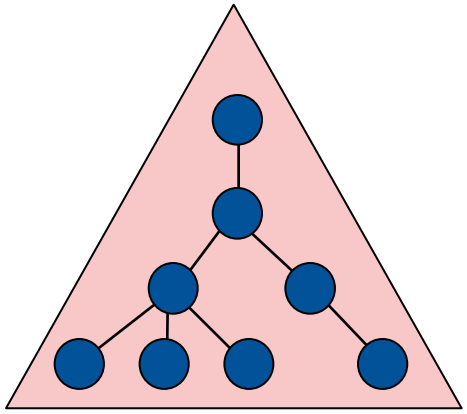
Highlights of HIPAA's Technical Security Services & Mechanisms

HIPAA Requirement	Applicable Solutions	PKI Applicable?	PKI Required?
Entity Authentication	ID/password Biometric, Token	✓	
Access Control	Firewall, PMI, SSO, LDAP		
Message Authentication and Integrity	Digital signature, Checksum, CRC	✓	
Encryption Over Open Networks	SSL, Triple DES, VPN, ebXML, S/MIME	✓	
Audit Controls	Application-specific and NSM, ITD, CCOW		
Event Reporting and Alarms	Firewall, NSM, ITD		

Transport Services

Transaction Zones: Best Practices for E-Health Migration





A directory is a special type of database optimized for high-performance read operations and scalability.

LDAP is a access methodology used to read/write directory information over TCP/IP.

X.500 is a set of standards that define access, interoperability, schemas, and scalability specifications for directories.

UDDI is "a 'meta-service' for locating Web services by enabling robust queries against rich metadata."

Directory Services
X.500 and LDAP

In comparing and evaluating X.500 vs. LDAP it is important to define the context in which the assessment is being performed:

- As differing directory access protocols, DAP vs. LDAP
- As a basis of differing directory architectures and standards (open vs. proprietary)
- As a basis for interoperability between directories

X.500 is a set of ISO standards used to define the model and protocols for implementing a global directory service. The standards define how clients can access a directory service (server) to obtain information, as well as defining standards for directory server-to-server communications to manage distributed directory functions. The standard also defines the information model (the schema) used to implement directory.

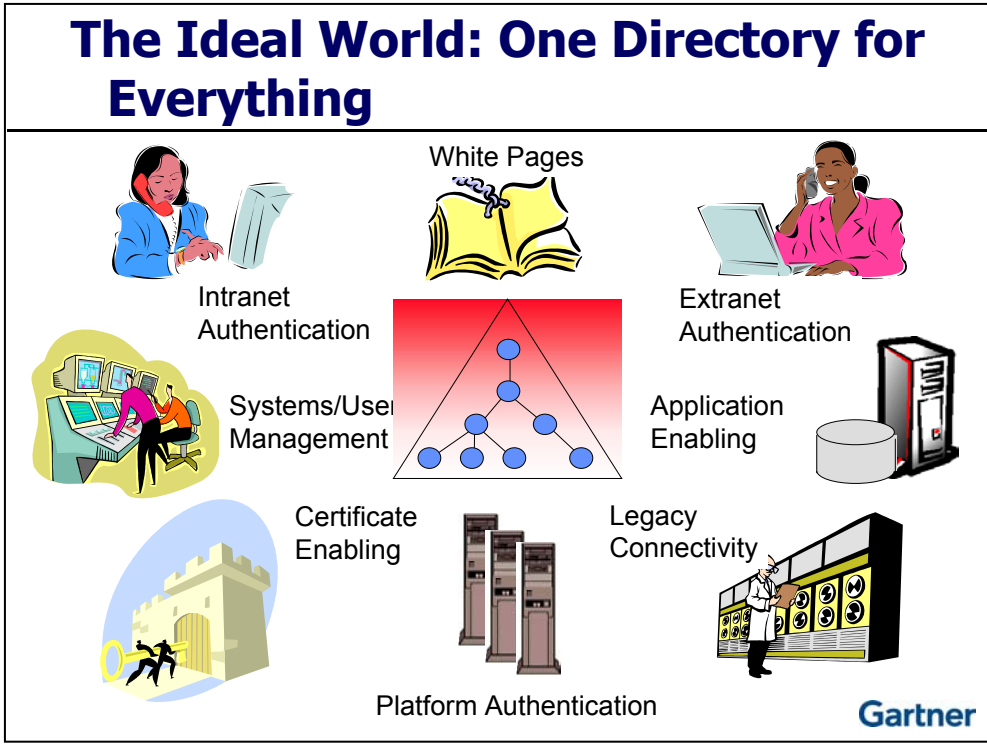
LDAP was originally developed as a subset of the X.500 directory access protocol (DAP) to provide a simple, and easy to implement protocol to access information stored in X.500 directories. Today, LDAP is used a standard to access all types of directories (X.500 and proprietary), and is being extended to more complete directory functionality through specifications such as *slurpd* - the replication model for LDAP.

Directory Services
The Vision of a Single Directory

The vision of a single enterprise directory to manage all aspects of the enterprise is compelling. Under this vision all users (internal or extranet), platforms, and applications authenticate to a common directory. Furthermore, the directory provides a single point of management for PKI certificates, desktops, servers, printers, network resources (including QoS), and business application data (including white pages).

The technical and business benefits of having a single directory are strong. New applications (intranet or extranet) can be deployed quickly. New employee productivity is increased because access rights are granted when a new user is defined in the directory -- there is no lag time between starting work and accessing business applications and resources. IT administrator overhead is reduced because adminstrators have a single point of management for a wide variety of IT functions. Business managers gain better control of their resources because the directory keeps track of employee information and assets. And these examples are just the tip of the iceberg.

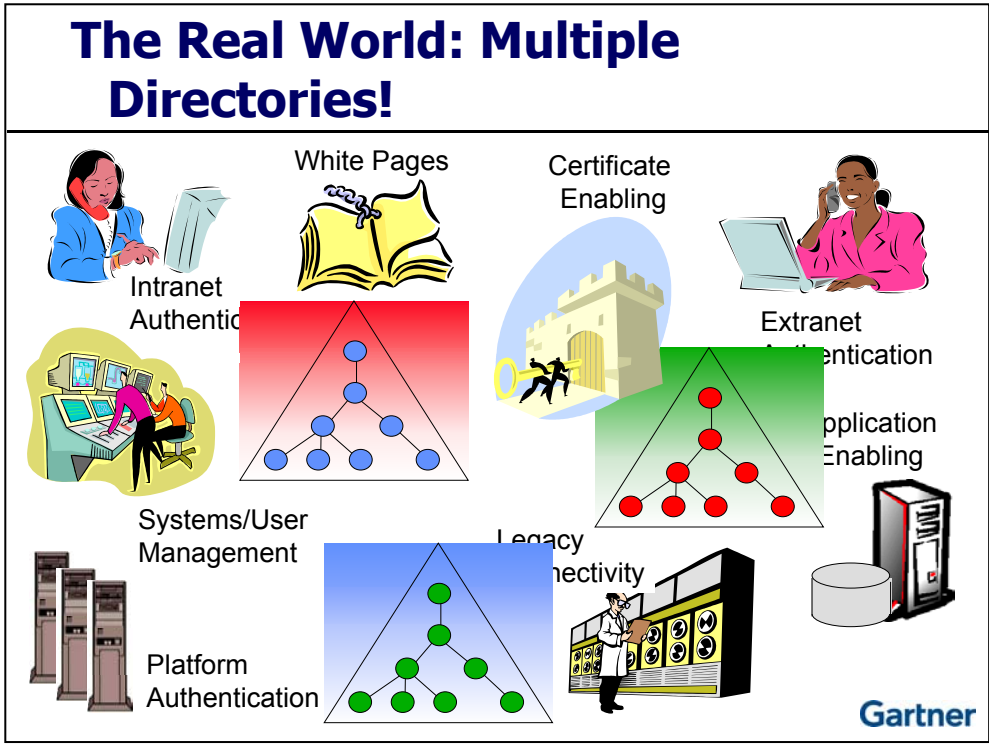
Thus the vision of one directory is utopian in nature -- perhaps too good to be true.



consulting

Directory Services
The Real World

The real world is far less perfect than the utopia of one directory. The more diverse an enterprise is, the more likely it is to have multiple directories. In this context we need to be clear in our definition of "directory." By "directory" we mean a data structure that describes the characteristics of a user -- this can include application information and security information. Thus our definition takes into account conventional directories (e.g., Active Directory, NDS, X.500, and LDAP directories) but it also embraces application-specific data structures. These structures might be contained in files or databases and used by applications such as e-mail, human resource management, CRM, supply chain, and more. This definition of directories opens the door to an increased count of directories in an enterprise and it blurs the vision of one directory.

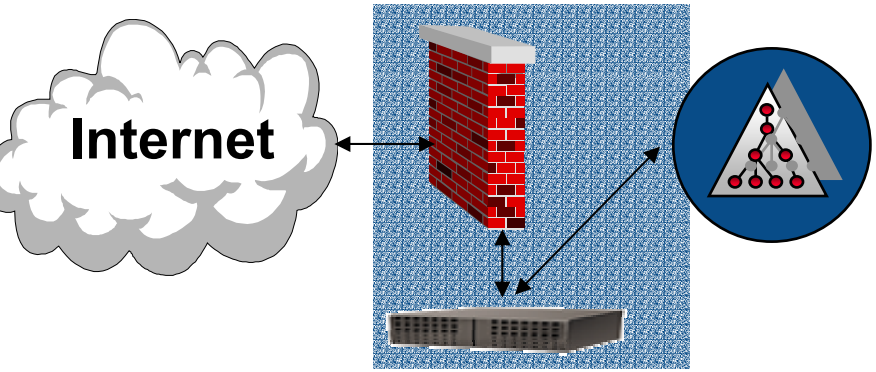


Although one directory remains theoretically desirable, it becomes more difficult to achieve under a looser definition of directory. The four inhibitors to directory unification are: (1) platform dependencies (e.g, Active Directory in Windows 2000), (2) explicit application dependencies (where applications only support one directory), (3) implicit application dependencies (where vendors only support top tier directories), and (4) suitability for task (e.g., high scalability, real-time performance).

Action Item: Enterprises should set expectations with their directory projects. A single directory is not achievable in the vast majority of cases.

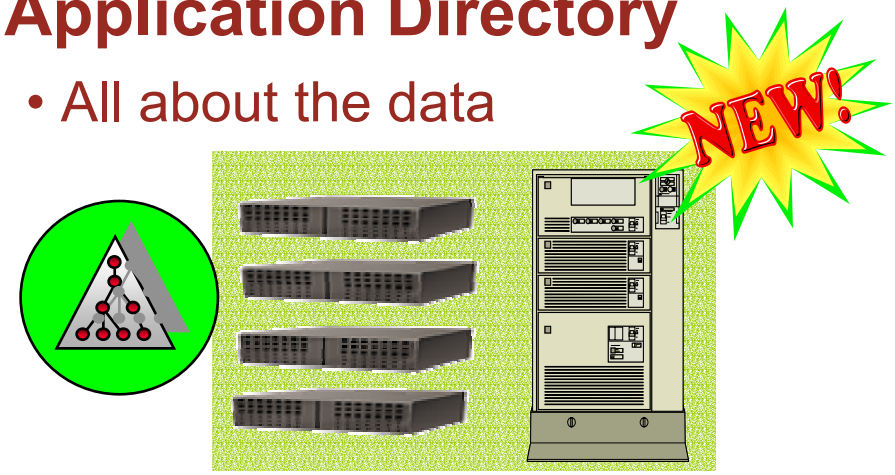
Extranet Directory

- All about performance/scalability



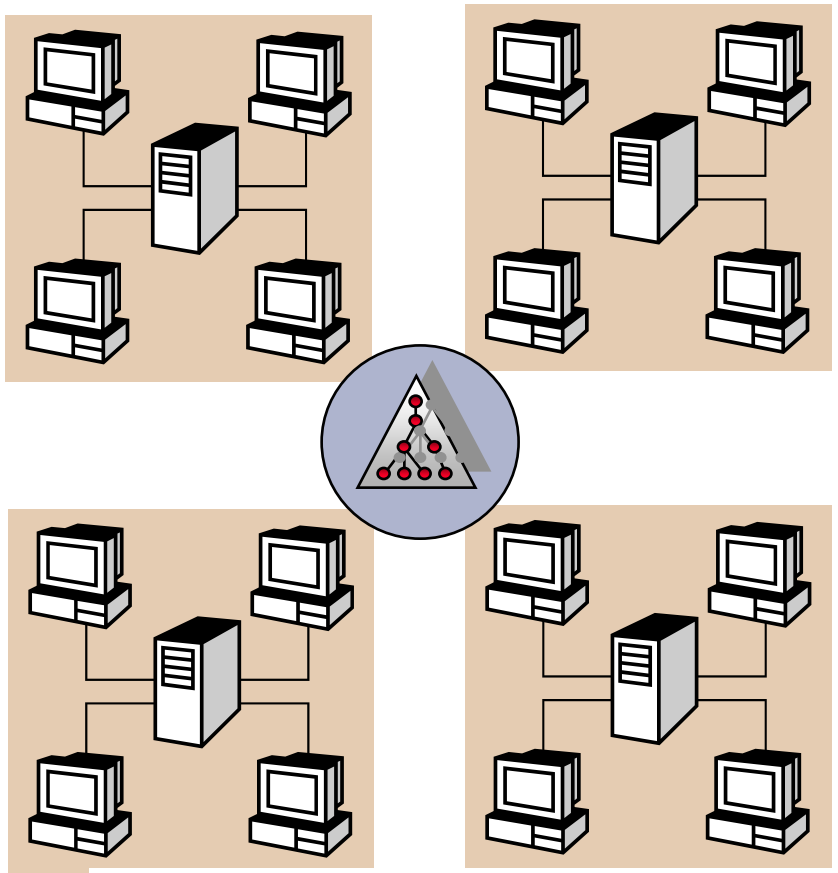
Application Directory

- All about the data



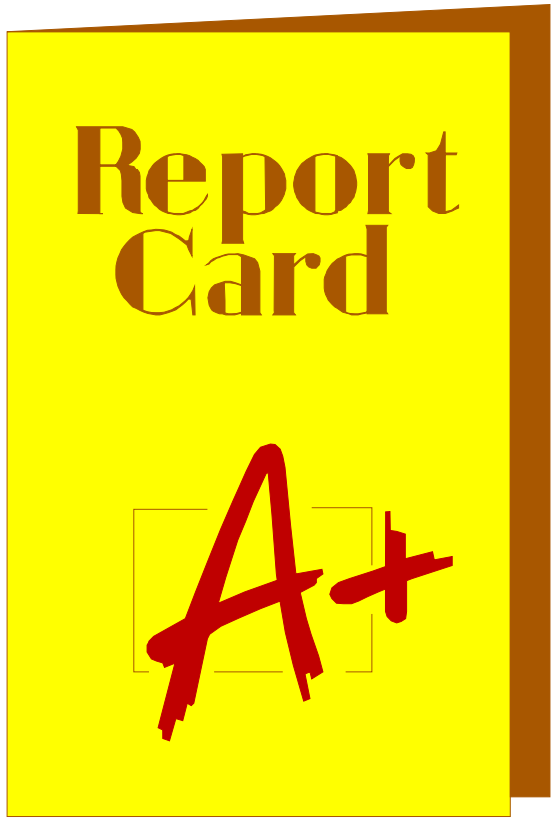
Network Operating System (NOS) Directory

- All about local login



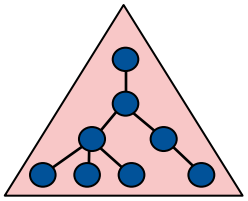
Directory Services
Directory Selection Criteria

- ✔ Support for LDAP v.3
- ✔ Schema architecture/security
- ✔ Application developer environment
- ✔ ISV support/enthusiasm
- ✔ Ease of use (install/maintain)
- ✔ Size of installed base
- ✔ Scalability/performance proof points
- ✔ Cost/licensing model
- ✔ Availability of professional services
- ✔ Bundled synchronization tools
- ✔ Replication methodology
- ✔ Support for standards (X.500, LDUP, LDIF, DSML, etc.)

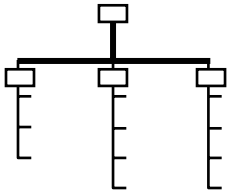


Directory Services
Metadirectory Products

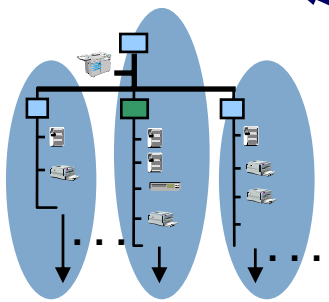
- ✔ Single point of administration
- ✔ Data accuracy and precedence
- ✘ Password synchronization
- ✘ Single sign-on



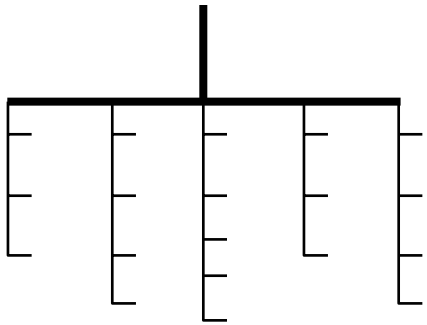
Active Directory

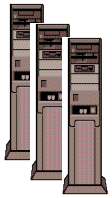


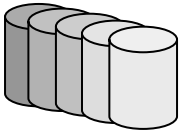
Generic LDAP-enabled directories (e.g., Netscape)



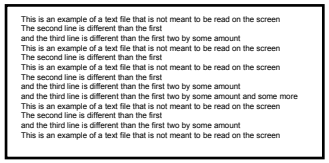
NDS



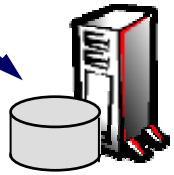




Oracle, Microsoft SQL Server, DB2 native access or ODBC



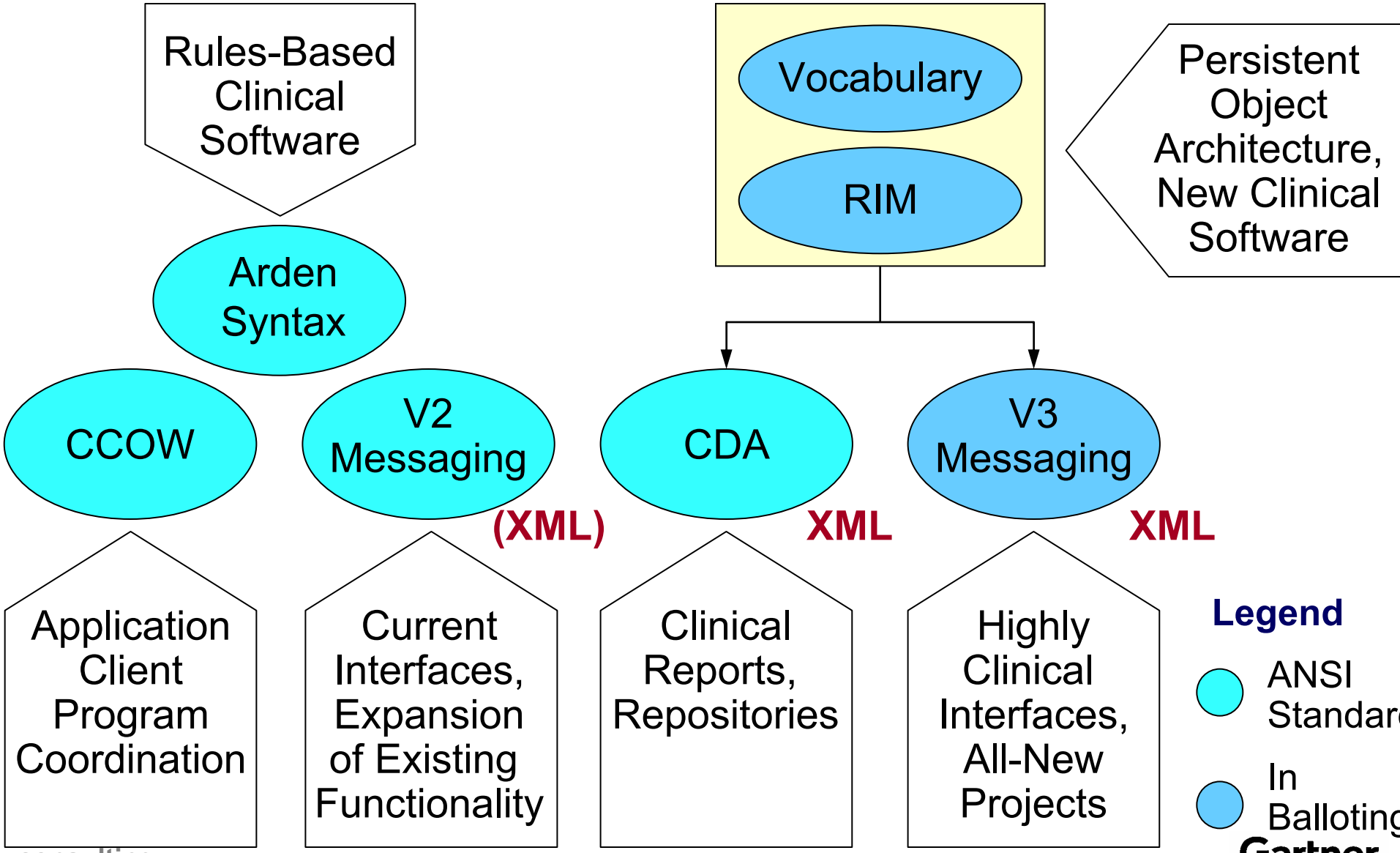
Generic text file



ERP (e.g., PeopleSoft and SAP)

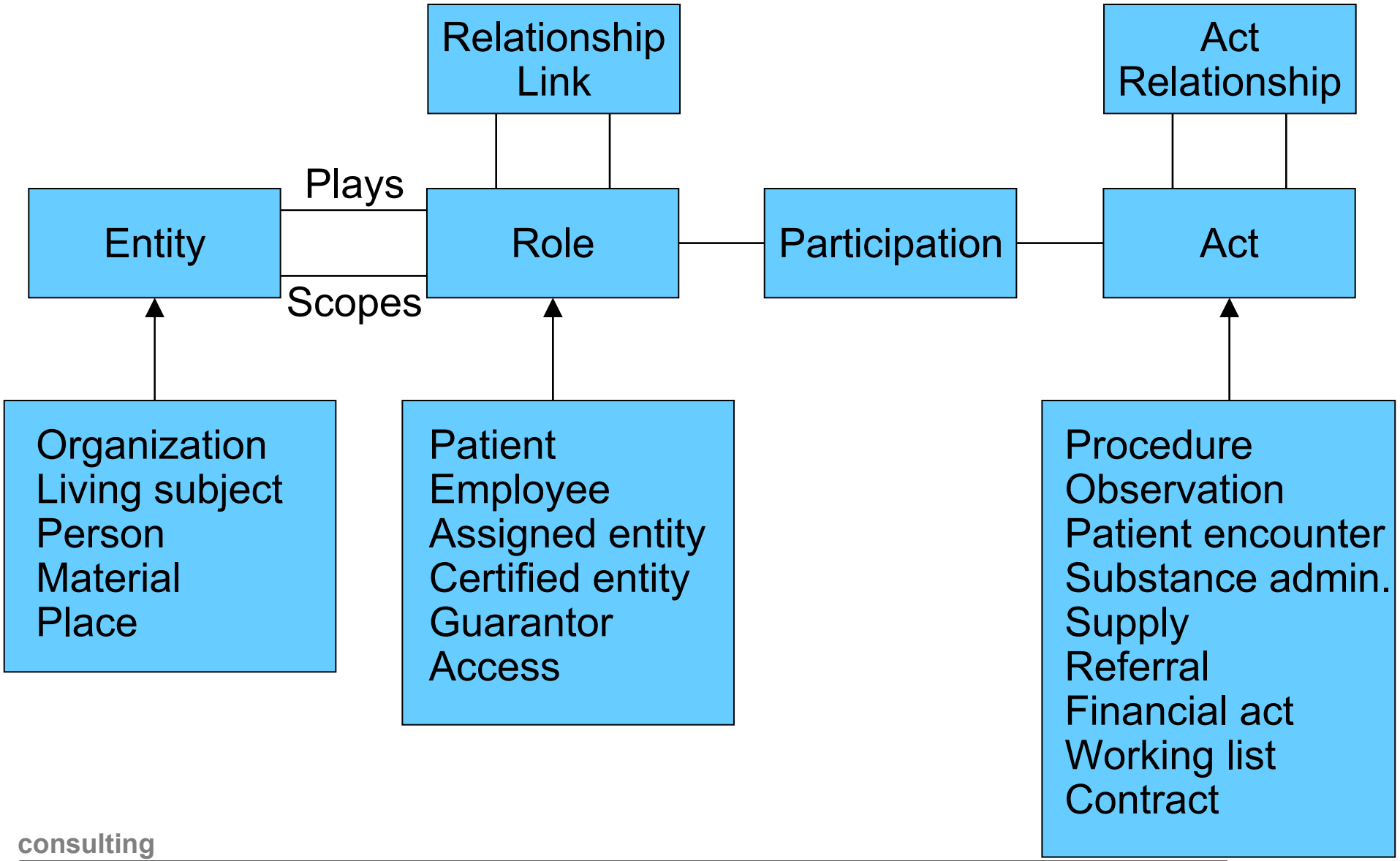
HL7 Messaging

HL7 Standards and Their Uses



HL7 Messaging

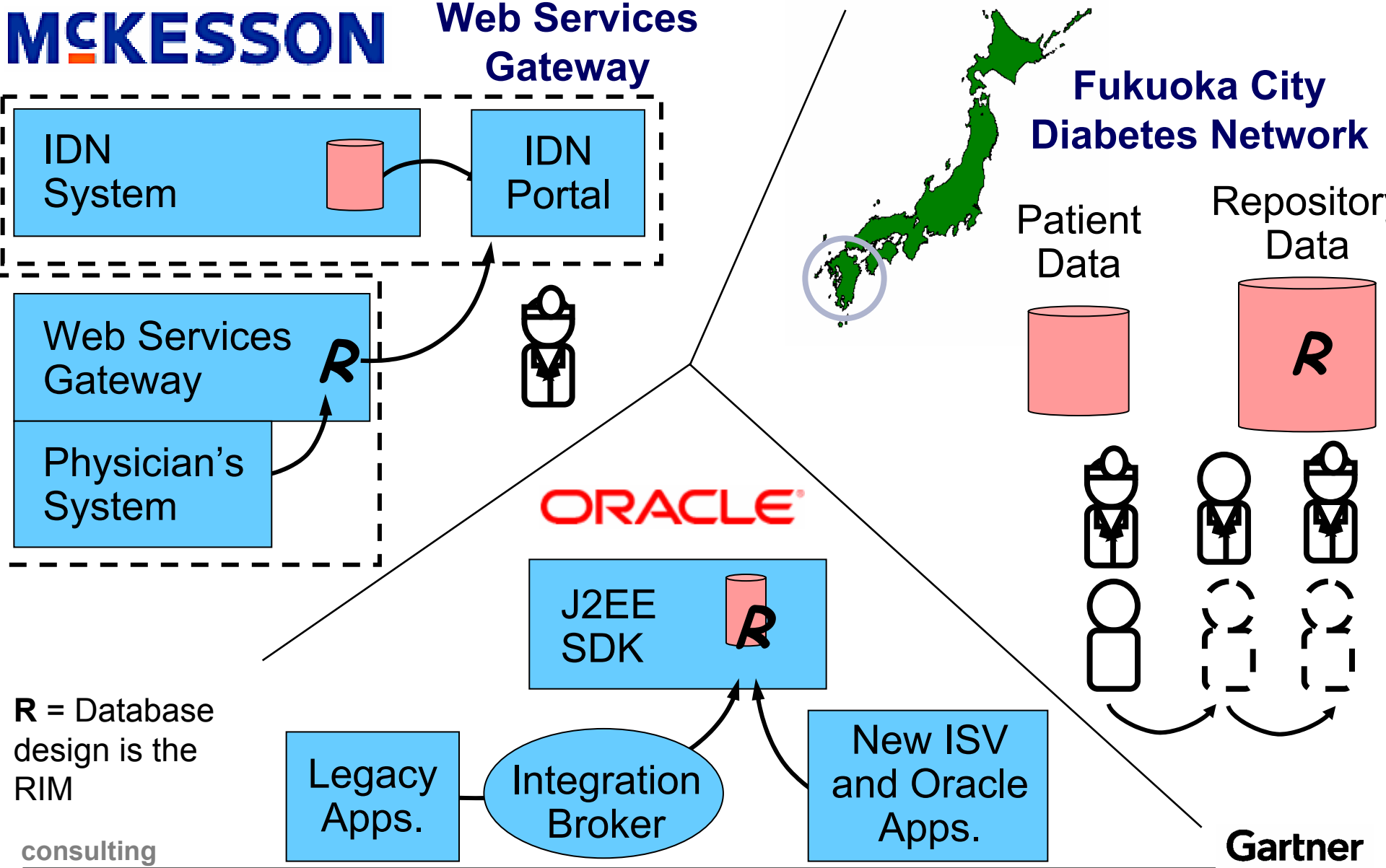
HL7 Reference Information Model



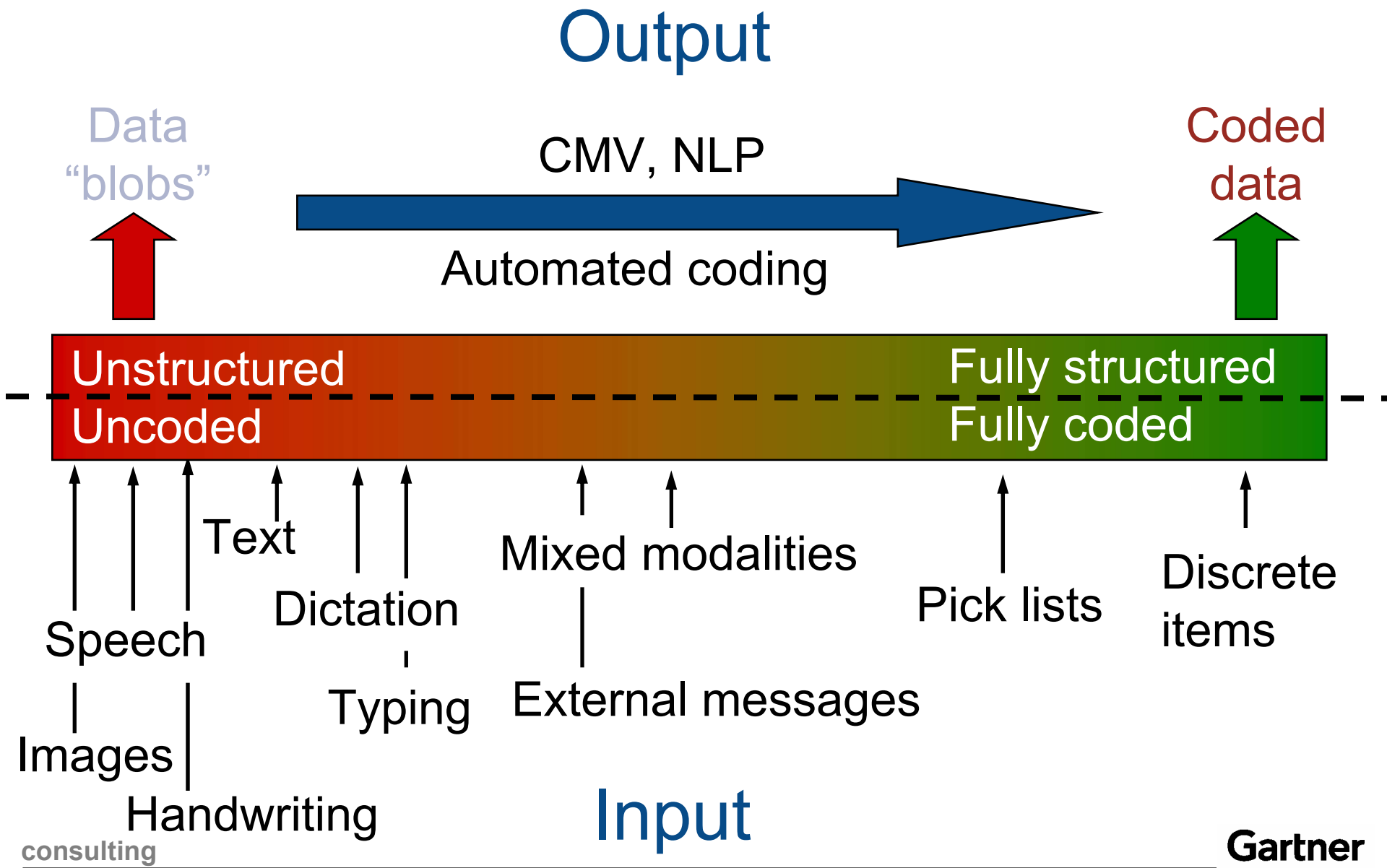
HL7 Messaging
Some National-Level Initiatives

- **Australia**
  - HealthConnect: National secure infrastructure, HL7 v.2 messaging, evaluating the GEHR
- **Canada**
  - Pan-Canadian Electronic Health Record (consolidation of provincial efforts for registration and sharing administrative data)
- **New Zealand**
  - Centralized national patient master index (HL7-based); evaluating HL7 CDA for text-based discharge and referral messages
- **United Kingdom**
  - GP2GP exchange of medical record info; XML messages derived from HL7's RIM
- **United States**
  - HIPAA Attachments, CDC NEDSS (public health surveillance), CMS VISION (ESRD outcomes)

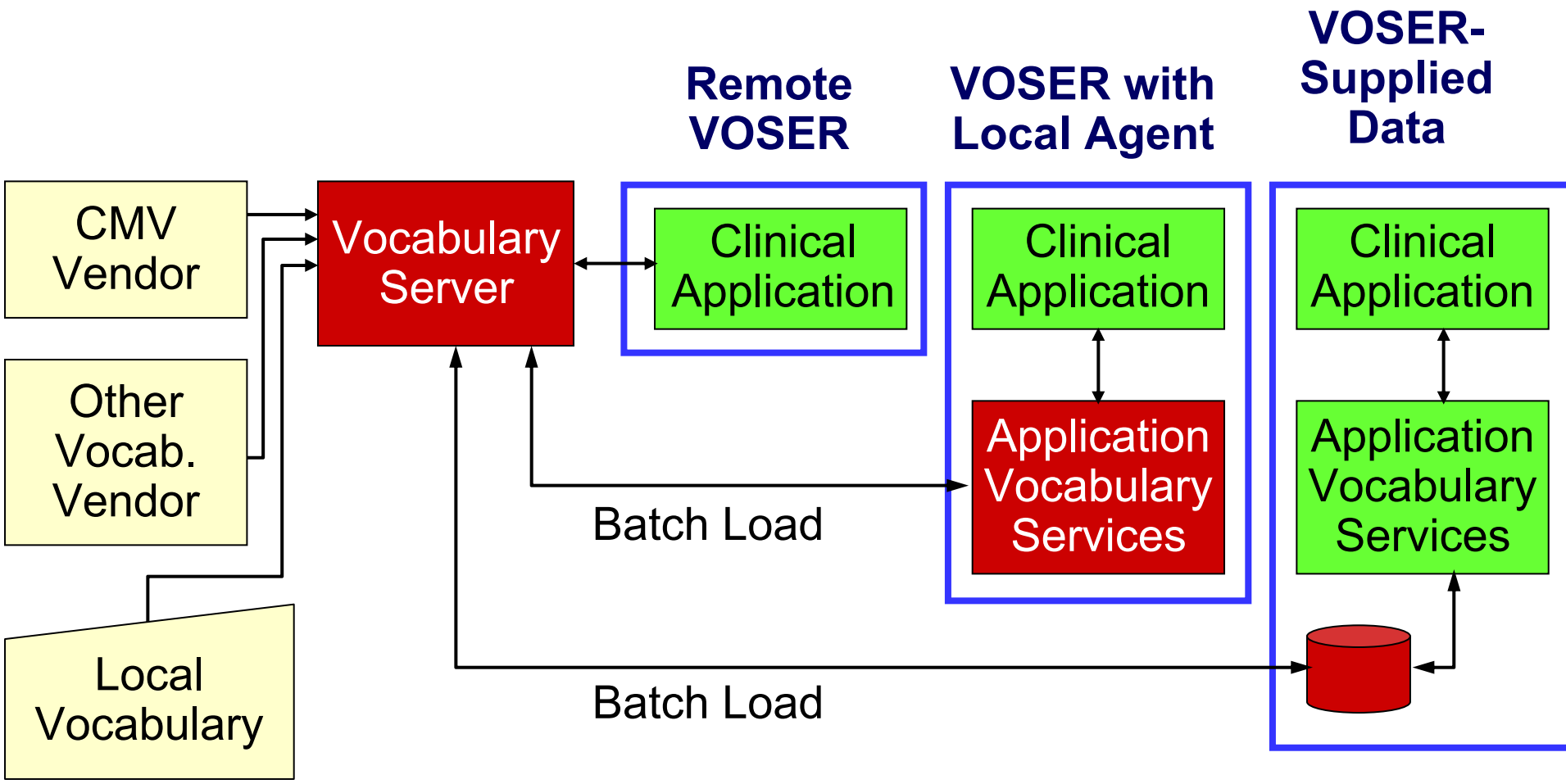
HL7 Messaging
Designing on HL7's RIM



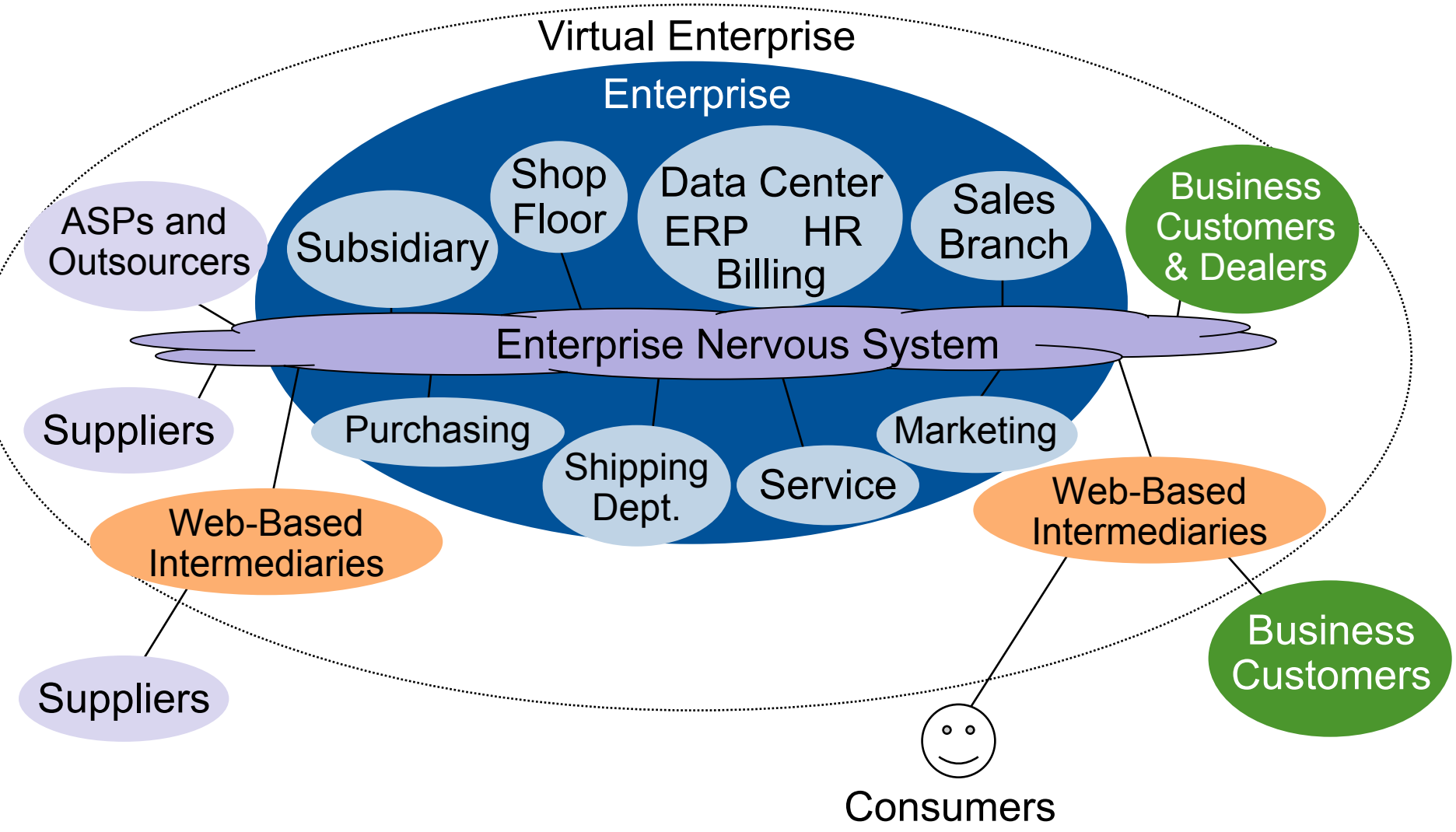
CMV Contribution to Error Reduction



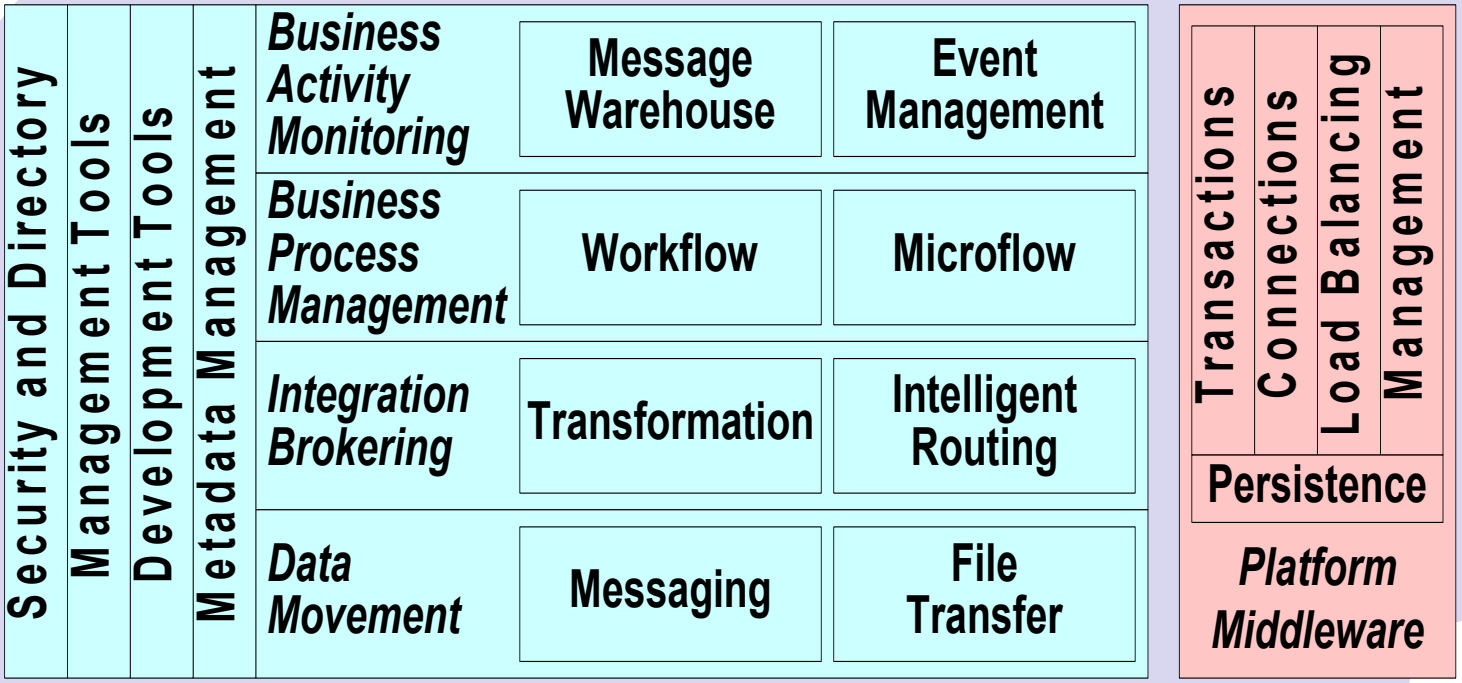
VOSERs: Key to Interoperability



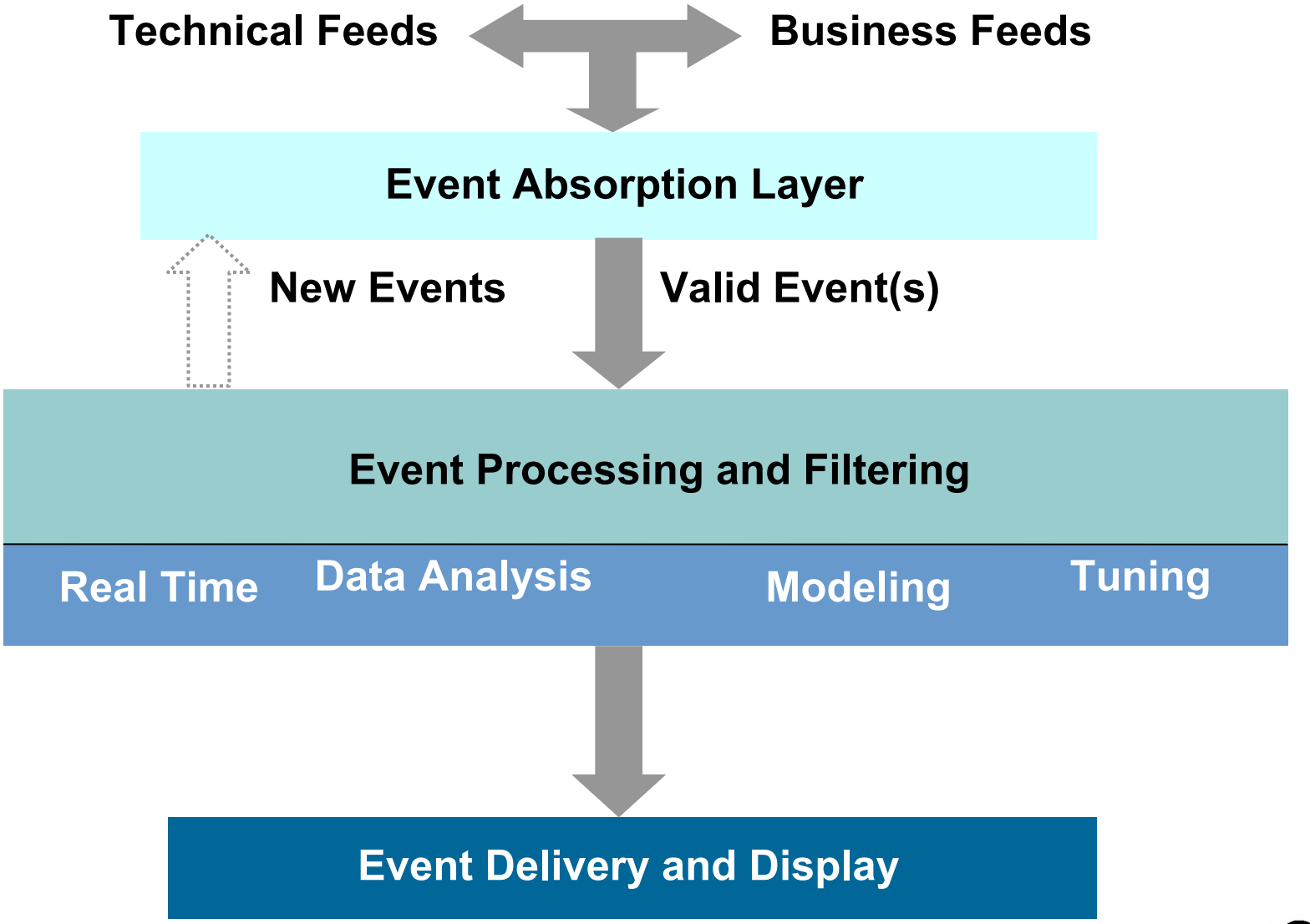
Business as a System



Enterprise Nervous System



BAM's Logical Architecture



Gartner

research consulting measurement community news